Documentation for the add-on to Tails

Author	:	swtor00@protonmail.com
Date	:	16.11.2025
Version	:	Release 0.90 / needs Tails 7.2 or higher
Licence	:	GPL 2.0
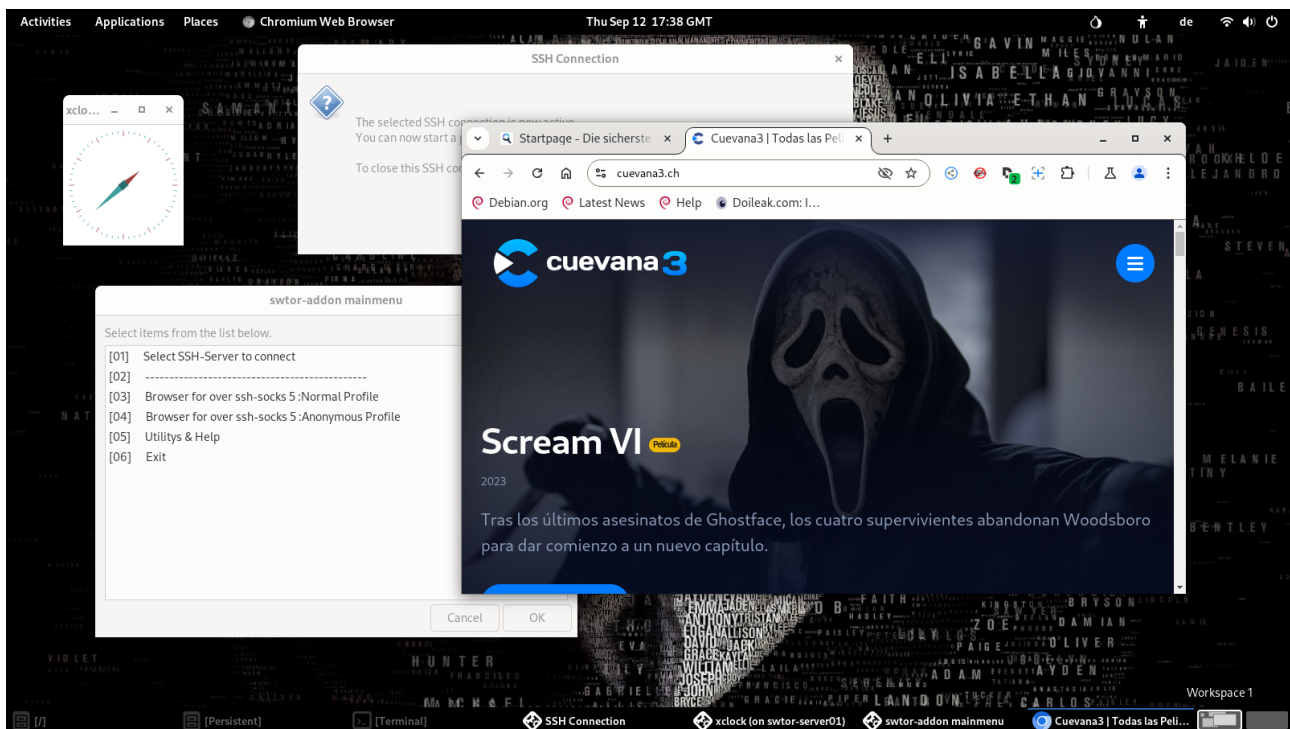
In the year 2017 I began to write the first implementation of this script for my personal use only. This first implementation was a very huge shell script and was running with Tails 2.2 in the background. My first attempt for this script was not for browsing Tor unfriendly Sites. I was using Tails almost everyday and as soon I received a call from a customer I had to shutdown Tails and boot my installed Windows System where all the Customer VPN's are stored. At the end I was tired of rebooting every half hour to work only for a couple of minutes and then reboot again with Tails. With the outgoing SSH-connection I was able to help my Customers (over VNC-Viewer or rdesktop for Linux) even If I was directly inside of a Tails session. At this point I began to realize that this ugly first script also could be used to visit multiple Websites without blocked services or even "captcha terror" because I was using Tails.

This first shell-code script was growing fast and ended in a little mess to extend and maintain as well. And, yes ... it was ugly to use and not very well integrated into Tails. Prior to version 3.8 of Tails, it wasn't possible to install software over the GUI. It was possible for me to implement this feature on the terminal only. My first script was only a terminal based shell script presented without any fancy GUI. The source-code was not openly available to the public. In the year 2018 I published the code under a free license on github.

With the current version 0.90 of the add-on, the monster script that I started with version 0.0.1 has become a bit more user friendly.

- A GUI based menu-system that even a Tails beginner or Linux novice can handle.

- Better integrated into Tails than ever before. Since release 0.83 it is even possible to autostart and initialisize the addon with activated DOT-files.

- Build a local socks5 server and make a SSH connection to a foreign host over the Onion-Network. This cheap little trick allows us to visit tor-unfriendly websites inside of a running Tails.

- Easy backup and restore of a complete persistent volume of a Tails USB stick.

- Can be upgraded over git on the fly ...

Have fun with my little add-on to enhance your user experience with Tails.

Best regards
swtor00

1.0 Introduction

This documentation describes how to install and use this add-on for Tails-Linux. You may ask yourself, why do I need such a add-on for Tails ? The Tails Linux system already protects your privacy by using the Onion-Network on every startup in the background. It is also true that a Tails system already makes a very good job to hide your true identity and the real WAN IP-Address to the websites you are visiting. To be honest, this job is much better done by the people behind the Tails OS and their supporters that anyone else could do it alone by installing the TOR-Browser bundle on a regular Windows-Computer or a Linux-System. If I would be very ironic, the only real purpose for TOR-Browser for Windows is to downloading Tails and configure the USB.

Although, it seems today en 2025 many Tor-Browser and Tails-Linux users are having difficulties surfing and navigating the regular World Wide Web (sometimes also called the Clearnet Internet like google and facebook as a bad example) , as some websites have set up discriminating rules against people who are using the Tor Browser to browse the web. At any specific moment in time when we are using Tails or the Tor-Browser in general,our personal IP packets are sent through the Internet crossing 3 different Nodes to hide the origin where the packets came from.

The so called "Exit-Nodes" of the Onion-Network can easily and instantly be detected as soon as someone queries with any remote IP Address from the URL below.

https://check.torproject.org/torbulkexitlist?ip=1.1.1.1

Therefore it is no longer a hidden secret to any visited website, that we are using the TOR-Browser or even Tails and they will often run this act of brainless "captcha terror" against regular users of the Tor-Browser. Right after here, you see a example of this so called "captcha terror".
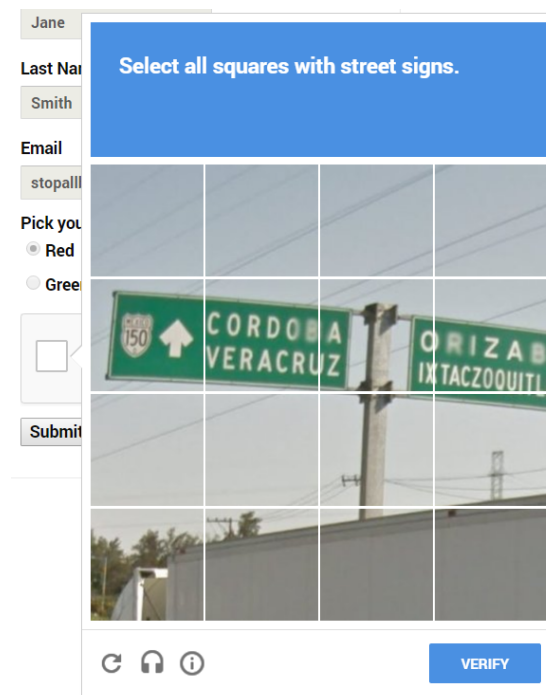
Alarmingly, the number of websites that even completely block or run the "captcha terror" against regular Tor users is growing in numbers day by day, to the detriment of Tor's usefulness.

Integrated inside of every Tails installation on a CD or USB medium, there is still the so called "Unsafe Browser". Because this "Unsafe Browser" doesn't make any use of the Onion-Network that Tails provide in the background, all data communications from this "Unsafe Browser" can easily be logged by your internet service provider (ISP) or your government or any Network Administrator from a Hotel as example. After Tails version 4.8 was released,it was not longer possible to start the "Unsafe Browser" inside of Tails. After Tails 6.0 was released, it was again activated by default.

It may only make sense to use the "Unsafe Browser" inside Tails solely to browse a captive portal like it is used in many public WiFi networks or hotels for connecting, but not really for more than this simple task. In next URL you may find some other useful Information about "Unsafe-Browser"

https://tails.net/contribute/design/Unsafe_Browser/

As I said, the "Unsafe Browser" is activated again since the release of Tails 6.0.
I highly advice you to disable the start of "Unsafe Browser" in the Greeting-Screen of Tails.
Please activate this very useful setting to see this Window if you try to start "Unsafe Browser" !!!
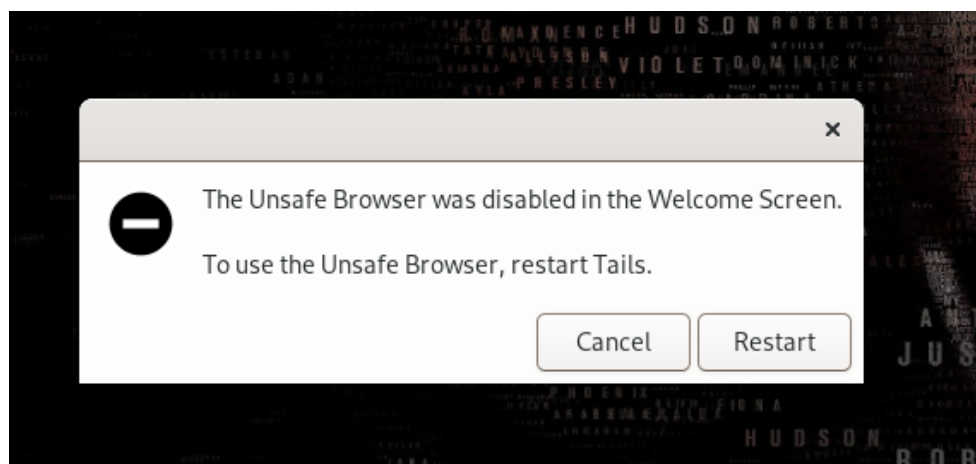
- IF YOU DON'T NEED THE UNSAFE BROWSER OF TAILS ...PLEASE DO NOT LET IT BE ACTIVATET IT IN THE WELCOME-SCREEN OF TAILS AND NEVER USE IT UNDER ANY POSSIBLE CIRCUMSTANCES !!!!

- AT THE SAME TIME YOU ARE USING THE UNSAFE-BROWSER OF TAILS AND VISITING A EXTERNAL WEBSITE ANYWHERE ON THE INTERNET→ YOUR REAL IP OF YOUR CURRENT USED WAN INTERFACE WILL BE LEAKED IMMEDIATELY TO THE REMOTE SITE !

Some smart people even try to start a VPN connection with OpenVPN or something similar to hide the fact that they are using the Onion-Network ,which can be blocked by any website or even an ISP.

Apart from the fact that you are only able to use a TCP port for a possible VPN communication (all UDP ports including ICMP Messages inside of Tails are blocked by default), it produces many more problems than it would solve.

In the endless debate in multiple forums on the Internet about the use of a Virtual Private Network (VPN) inside of Tails, I recommend to read the following URL completely.

https://gitlab.tails.boum.org/tails/blueprints/-/wikis/VPN-support

The developers of Tails (and they know Tails from the ground up with every little detail that other so called technical experts don't even know yet or ever have learned) have a loud and clear statement to integrate any kind of a software like OpenVPN into Tails Operating System.

- NO NO NO and a big NO again !

The only clean and acceptable way for the multiples of developers of Tails to have a fixed outgoing IP address (that is not part of the Onion-Network of course) is to create a local socks5 Server and to build a SSH-Connection to a remote Host.

Now, exactly right here, my special add-on for Tails enters the game called "Enhancing Tails with a kind of VPN," and provides some very useful functions for the many Tails users out there.

- Use of an encrypted SSH-connection to a remote host and building of a local socks5 proxy. Even the traffic that is sent over the so called "Exit-node" of our communication is still encrypted until it reaches the destination SSH-Server. When the connection packets leave the SSH-Server to any external website for example, the packets are not longer protected by SSH itself and would look like any normal network traffic from a standard Desktop computer running with Linux.

- All SSH traffic is encrypted and routed over the Onion-network, as long you are using an SSH server anywhere on the Internet. If you are using a SSH Server in your own network at home, only the connection from your Tails system to the internal SSH server is encrypted. And I assume that this is not the way you would like to go about hiding the fact that you are using Tails.

- A local Browser (Chromium) with three different profiles that can be used to visit TOR unfriendly websites like youtube.com and many others that would block regular TOR users like second class internet users. All three Chromium profiles are protected against multiple actions like Web RTC and multiple other trackers in general.

- All local DNS resolution traffic on UDP Port 53 for Chromium is routed over the local socks5 proxy to the remote SSH server . This means you never contact your local DNS server from your currently used network or ISP, like you would do with the activated "Unsafe Browser" of Tails. And I say it again, just as a very important reminder. Do not activate the unsafe browser !!

- For any particular website that we are visiting with Chromium on the Internet, it is no longer possible to detect that we are using the so called "Onion-Network" to hide our personal information, or even more important our current public IP-address at all. All the traffic that the owner of the website can analyze, is coming from the regular public IP address of the remote SSH server we are currently connected to.

One real huge problem still remains with using the Tails system to contact onion-unfriendly systems at all. It makes no difference what kind of working bypass protocol we are using to hide the fact that we are using Tails in the background. These so called bypass systems could be done by one of the following 3 techniques.

- Possible Bypass System 1 (Using SSH to build a local socks5 Proxy)

This is exactly the way this add-on works and is the preferred method by developers of Tails. The add-on itself only use already installed Tails software to create our secured SSH connection.

- Possible Bypass System 2 (OpenVPN Server with a single TCP port)

OpenVPN is a very popular software for creating any kind of VPN. Most of all public OpenVPN servers on the Internet (there are multiple thousands of them on the net) only work with a single UDP port to connect. The UDP protocol is multiple times faster than the TCP protocol. This is one of the main reasons, why so many OpenVPN servers only providing UDP ports for connecting. There are not so many OpenVPN servers out there on the Internet, that can be used with the TCP protocol. Please take a closer look at the OpenVPN Servers on the following URL and you see what I mean. Almost 98 % of all servers only provide UDP ports for connecting.

https://www.vpngate.net/en/

This very accurate list shows multiple free OpenVPN Servers worldwide. I use this impressive list of free OpenVPN servers very often to watch live TV and read some newspapers from my current location while I'm on vacation, because every connection attempt from a foreign Country is blocked inside my own Country where I live. I use this list very often with a OpenVPN client under Linux or even Windows. But not within Tails, for a few several understandable reasons.

It is one thing to only watch a harmless TV show over a public VPN server that is managed by a person that I don't know in person and log all my connections over this server, but it is a completely different kind of story to send any kind of sensitive data to a server that can be trusted for 100 %.

- Possible Bypass System 3 (proxychains)

With my first experiments with Tails to establish a stable connection to a few TOR unfriendly websites I was using this tool called proxychains. Sometimes it worked for me more or less not too bad but a half hour later the program stopped working without any clear reason to me. In my humble opinion it wasn't the right tool to do the job properly. You may test it for yourself, you may come to a different conclusion than me.

https://forkdrop.io/installing-and-using-proxychains-utility-on-tails-live-boot

The following 3 very often used VPN protocols don't work inside Tails.

- LL2TP
- IPSec
- WireGuard

All of the above listed well known protocols are using or are depending of one or multiple UDP Ports to work properly. Inside Tails it isn't possible to create a simple UDP connection directly to the Internet.

A big Warning about using any of the 3 working presented bypass techniques including the remote ssh-servers that you are using with my own add-on here:

At this point I would like to raise awareness about the trust you are willing to give to a foreign host system and his administrators or users, which may could easily read your complete communication that would be sent through to the foreign server over Tails. If you would like to use any of the 3 working bypass techniques, please don't underestimate the control they have over you in the exact moment in time that you are using their servers.

Almost any VPN or SSH Service provider (commercial or free) worldwide out there on the Internet make claims on their websites with really cheap marketing statements like the following ones:

"We don't log anything !"
"We don't spy our users !"
"We protect the privacy of our customers !"
"You can trust our VPN Services !"

To be honest. That's in the most cases only cheap marketing crap for foolish customers, that truly believe that marketing bullshit published by the company who offers the Service. Some very interesting articles about the so called "no-log policy" of some important worldwide VPN providers can be found right here.

https://www.theregister.com/2011/09/26/hidemyass_lulzsec_controversy/
https://www.pcmag.com/news/7-vpn-services-found-recording-user-logs-despite-no-log-pledge

If you read the above article carefully, you may come to the final conclusion that you shouldn't give your personal trust out to the first person or company who offers you a VPN or a full SSH account for free. Even if you pay for a service with a monthly fee, there is no guarantee that you aren't being "tracked" by this VPN server or any other active users of the remote system. Some very insane and shameless VPN providers do make a second business with selling the collected VPN data to other company's for marketing purposes. The Company Avast as a very horrible example was selling over years the costumers VPN data !!!!

If we are talking about the trust you are willing to give to a company or a remote server, we should also talk about one of the securest email providers out there on the Internet called Proton-Mail that reside in Geneva / Switzerland.

The company Proton also claims until the year 2021 that no log files are generated. The french customer of Proton mail who was arrested 2021 by the police, may see it completely different. He was using his free Proton mail account over the normal URL of the Clearnet Internet instead over the onion address that Proton provides for the customers. If this french customer of Proton had used the TOR-Browser to access his mail, he would still be free.

https://account.protonmail.com

This was the URL of protonmail he had used prior he was arrested.

Proton gave the french police department the public WAN IP-Address he was using to get his personal mail. A few hours later he was arrested by police and wearing handcuffs. Be reminded again from me, when a company says to the public what they would never do ... they'll do it for sure, if they have to !

https://arstechnica.com/information-technology/2021/09/privacy-focused-protonmail-provided-a-users-ip-address-to-authorities/

If you are using Proton mail (I do it as well → swtor00@protonmail.com), my personal advice is clear. Only use the onion V3 address of Proton.

https://protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion/login

This means you should do this only with Tails ! .. and DON'T under any possible circumstances check your private Proton mail-account with a standard PC Operating System like Windows outside of Tails. In the same moment you are reading your Email outside of the Tor-Network you are visible with a public IP address to the Company Proton.

Prior to showing 3 possible working SSH scenarios with the add-on, we have to talk about the dangers of using it at all. From all the 3 described SSH scenarios in the next chapter, you should only use the last presented scenario (scenario 03) whenever possible.

- Never create a login with a username / email-address/ password that you have ever used on the standard internet at anytime.

  A special note about the above rule, if you are living in a country like China or something similar that complete blocks Gmail. For example, if you are the owner of a Gmail account, you would never have a real change to login over the TOR-Browser. With the help of the add-on, it would be possible to get a chance to Login for that particular Gmail account. That's maybe the only possible exception !!! If you don't need any access to a Gmail account during you are using Tails. Stay away from using Google.

- If you need a valid Email-Address to register for a service or something similar, while you are using Tails, you have to create a single Email-Address that you would only use inside of Tails and nowhere else.

  NEVER TRY TO ACCESS OR PUBLISH THIS SPECIALLY CREATED EMAIL-LOGIN TO ANYONE OUTSIDE OF TAILS !!!!!!!!

  NEVER SEND AN EMAIL FROM YOUR ORDINARY EMAIL TO THIS TAILS ONLY GENERATED EMAIL ADDRESS !!!!

  NEVER SEND AN EMAIL FROM THE TAILS ONLY EMAIL TO ANYONE THAT YOU EVER CONTACTED BY YOUR ORDINARY EMAIL SYSTEM AT HOME OR IN A BUSINESS !!!

- These kind of digital fingerprints (Emails / nicknames / passwords and many more little things that you often not think about) could be easily tracked back to you as a person with enough effort and time. Never use a Email-address for a possible password-reset in the future that directly points to you !!!

- Only use the add-on to solve problems with tor-unfriendly sites at all and if possible use every time the more secure builtin TOR-Browser of Tails to connecting it.

- You should never use a personal credit card to pay anything, that points directly to you.

- You never use any kind of 2 factor authorization that needs a mobile number to register. It would be possible to use "Google Authenticator" on Linux that also works offline. How to install this application is not part of this manual.

- Never use any websites simultaneously inside the TOR-Browser and the Chromium Browser used by the script. This is because in case your internet is going down, both of your connections will terminate at the same time, and it will not be hard for someone spying on you to recover the pieces and complete the puzzle. It may be better to use only one browser at any one time and not trying to mix them up.

- We are already in the year 2025 and we still have millions of dummy websites that still use these stupid old fashioned http:// instead of the secure alternative https://.
  You well know that TOR can be exploited using the vulnerabilities present at its exit nodes. So, if you access HTTP sites using TOR, there are chances someone might access your information while it is on the endpoints. The data transferred to and from an HTTP site is not encrypted and can be viewed at the endpoints as TOR only encrypts the connection inside its own network. You can prevent such situations by the use of HTTPS websites.

- HTTPS websites use end-to-end encryption protocols like SSL (Secure Socket Layer) and TLS (Transport Layer Security). So, all your data remains safe, even if it is outside the TOR network to the final destination.

- Never wait more than a few days to update the Tails system if ever possible. It is very important that you always use the latest stable release of Tails.

- Only use search engines inside both browsers that do not store personal settings in any kind. There are 2 known public search engines that do this, they don't store anything about your searches, and so far to date 2025 these two search engines haven't been caught doing this.

  https://www.startpage.com

  https://duckduckgo.com/

  If the new ONION Brave Search (since 2022) is collecting data, is not sure. We see it soon.

  https://search.brave4u7jddbv7cyviptqjc7jusxh72uik7zt6adtckl5f4nwy2v72qd.onion/

- Do not use and activate the unsafe Browser of Tails. Yes, I know this is the third Warning I gave you !

- Do not try to install any stupid P2P software like Torrent or something similar inside of Tails.

- Some people suggesting a increased security-Level for the TOR-Browser that can be set by the user anytime.
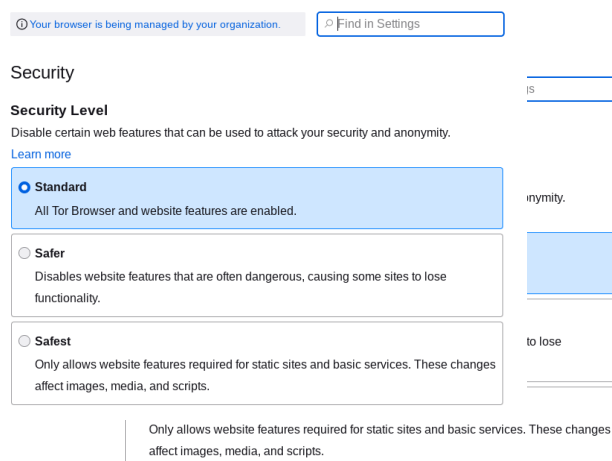
Be warned by me : If you increase the Level to the mode "Safest", almost any modern Website is looking horrible ugly and is more or less useless. I did never increased this Level during the long time I was using Tails.

- If you are downloading any kind of files with any of the 2 Browsers inside Tails (like any Microsoft Office Files as a simple example) , please don't try to copy them to USB and open them in a other Operating System like Windows with an installed Office in place. What you are downloading with Tails should only be opened inside Tails and never leave Tails. What happens in Tails → remains in Tails.

  https://www.thedailybeast.com/this-is-how-cops-trick-dark-web-drug-dealers-into-unmasking-themselves

  Some very stupid drug dealers downloaded a excel sheet from the Tor-Browser and opened this by the police manipulated excel sheet with their regular used Windows System. In the same moment as they opened the sheet, their public IP was transmitted directly to the police with the help of Office-Macros.

- Do not try to install the TOR-Browser Bundle on an ordinary Operating System like Windows or Linux and use the same credentials you created already for Tails only. If you really have to go this highly not recommended way, then you have to create new emails and SSH accounts for every system.

- Save the data from the persistent volume of Tails on at regular intervals. This backup should be placed on a very secure location inside your own residence or even better transfer the backup with SSH to a remote host in another country than your current one. And yes, with SSH you can copy files to a remote host as well. And when you need this backup, in case of a damaged stick (some call it a Tails emergency) , you need the following information to copy back the backup to a new Tails stick.

  - DNS name or IP address of the backup server
  - Port for connecting
  - username and password
  - Exact location of the backup inside the user-directory
  - You may also need the SSH-keys if you can not login with a password to the remote host.

  It would be very good practice to try out this "emergency-scenario" as long as you still have a working Tails. If you have a real "emergency" it could be maybe too late to copy the image back to a new Tails medium.

- Use a strong and long password for the persistent volume of Tails. Please take a little advice from me. Use a long password that you can type also with the standard American keyboard or you have to switch first the keyboard, prior to typing the password for persistence.

- Always try to shutdown the Tails-OS the clean way. If you don't shutdown Tails properly, the persistent volume could be damaged.

- If you are using Tails in public areas like a library or a restaurant, never simply walk away from the Computer running Tails with the unlocked persistent volume. The first action should be to "Lock" the running Tails. After you have "Locked" Tails , you can safely walk away.

- Never try to visit any Tails or TOR related Websites with a normal browser using a Windows or Linux System. This following websites especially.

  https://tails.boum.org
  https://www.torproject.org/
  https://gitlab.tails.boum.org/tails
  https://github.com/swtor00/swtor-addon-to-tails
  https://www.reddit.com/r/tails/

  You know, what the funny thing is about the reddit forum for Tails on reddit.com ?

  There are a lot of active Tails users on that forum that try to be as "Anomymous" as possible as long they are using Tails and the first thing they do is the following ... one reddit as a example ! They register for a new reddit account with a private or even worst with a business email-address for posting on that forum. Of course all done with an ordinary browser with a Windows or Linux OS. If you would like to visit this websites, please do it the right way and use Tails to visit them.

  Or maybe this one .... as a last very ironic example from me, how you shouldn't post a photo on reddit :

  You have a strange error message inside of Tails and you don't know what do with this message ? You take a photo of the error-message with your current smartphone and post this photo directly to the Tails forum on reddit . There are so many nice users of Tails in that forum, someone may know the solution to your problem right ? You are probably not aware of this, but the following worst case scenario can happen very quickly.

  - The serial and IMEI number of your smartphone are hidden in the Meta-Data of the photo that you made with your phone.
  - The exact location measured with GPS may also be included in the Meta-Data.
  - And last but not least , the same photo may also already be stored in a Google or Apple cloud depending on the OS by the used smartphone.

Please do not underestimate the amount of Information that could be hidden inside the Meta-Data of the following file types (only a few example).

- • Photos with multiple information like described above.
- • Generated PDF's that contain the serial-number or the Adobe Live-ID of the product used to produce this PDF.
- • Office documents may contain a serial-number/company name or even a Microsoft Live ID if you created the document with a Office 365 Account on a other computer.

Below you'll find a very good overview with multiple examples about the real danger of Metadata inside photos and PDF files or word documents :

https://www.metadatarisk.org/collateral/
content_security_risksUS_Brief_Dangers_of_Document_Metadata.pdf

Inside of Tails exist a little tool called Metadata Cleaner to remove unwanted hidden META data from multiple types of files. You find it under "Accessoir".
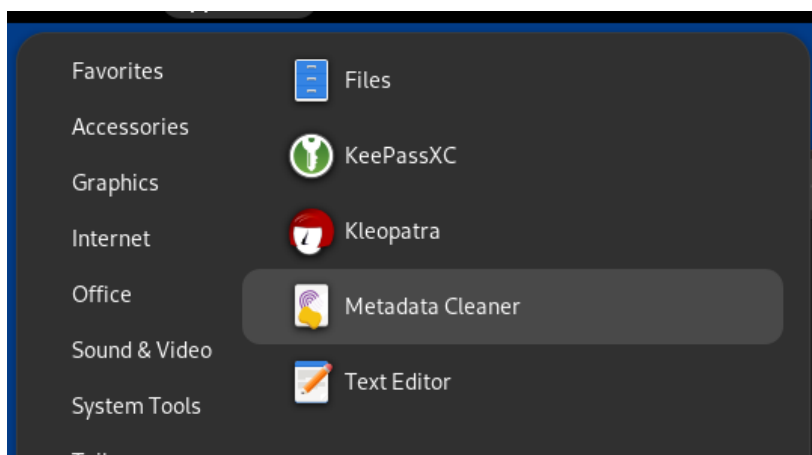

You may find all of my above security tips for using Tails in a secure way are way to ridiculous or excessive, but if you are living in a Big Brother Country like China with a very strong Internet censorship these tips and tricks may help you to stay free instead of being recognized and identified as a Tails user with all the possible consequences.

2.0 Using your own SSH server inside your own Network at home

For this simple and not really recommend scenario, you need at minimum, a second computer with Linux or Unix running on your own network at home. For this SSH-daemon you could use, for example, a simple Raspberry-Pi, or of course, any other computer with an SSH daemon would work as well. This could be implemented with a Linux System like Debian or many others without any problem. For a simple example to build a standalone SSH-server on a Raspberry-Pi I would recommend the following URL.

https://phoenixnap.com/kb/enable-ssh-raspberry-pi
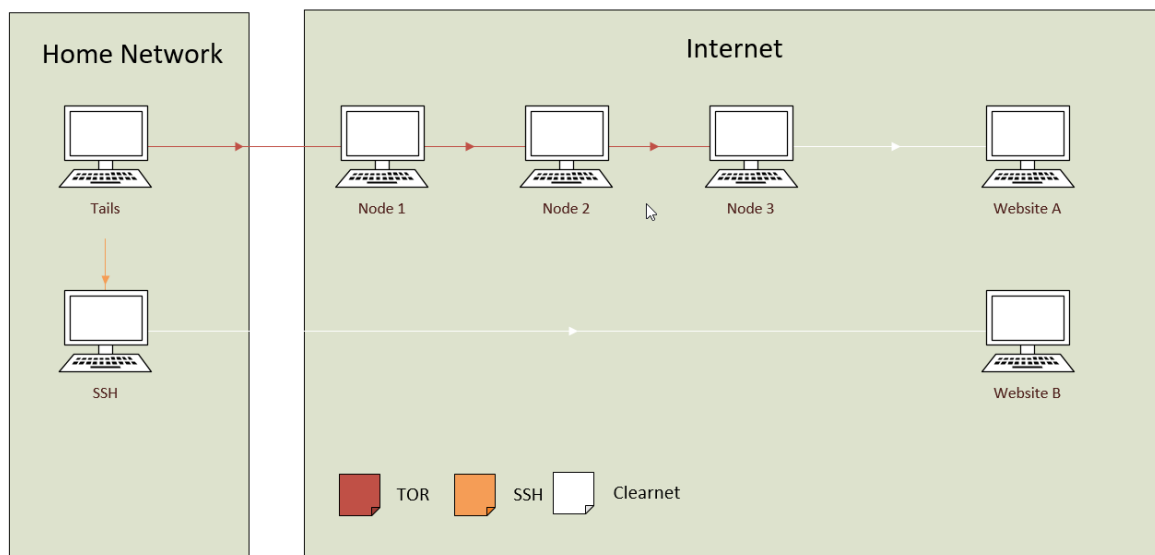
Scenario 01:

If you are using this "not so perfect first scenario 01", you can do the following:

- Use a Website like Google or many others that normally would block your connection as soon you are trying to use it inside of Tails. To be reminded again ! The complete Internet traffic (Data) that you send via my script through the Internet (from the SSH-server at your home to Website B for example → the white line in the graphic), can be tracked and analyzed by your current ISP, because it would be coming from a regular computer inside your own home network ! Only the websites that you are visiting with the TOR Browser over the Onion-network are secure to visit without to being tracked (Website A for example → the red line in the graphic). After the data is encrypted in the last node, the data leaving the exit-node of the onion-network, the network traffic is now showing again in the white color.

- Because the destination SSH-Server is inside the same physical network, the data you are sending from tails to this server aren't crossing the router into the direction Internet. These packets aren't routed over the 3 external nodes, because this network traffic is only local. Only the traffic from your local ssh-connection is passing the router into the internet.

  With the release of 0.83 of the addon for Tails and the new implemented redirection feature it would be possible to send all your local data encrypted over ssh to a remote host. In this particular case your ISP would only see the encrypted traffic to this remote server, but he can not track what your are doing exactly (because of SSH).

3.0 Using your own SSH-server that can be used when you are not at home

Scenario 02 :
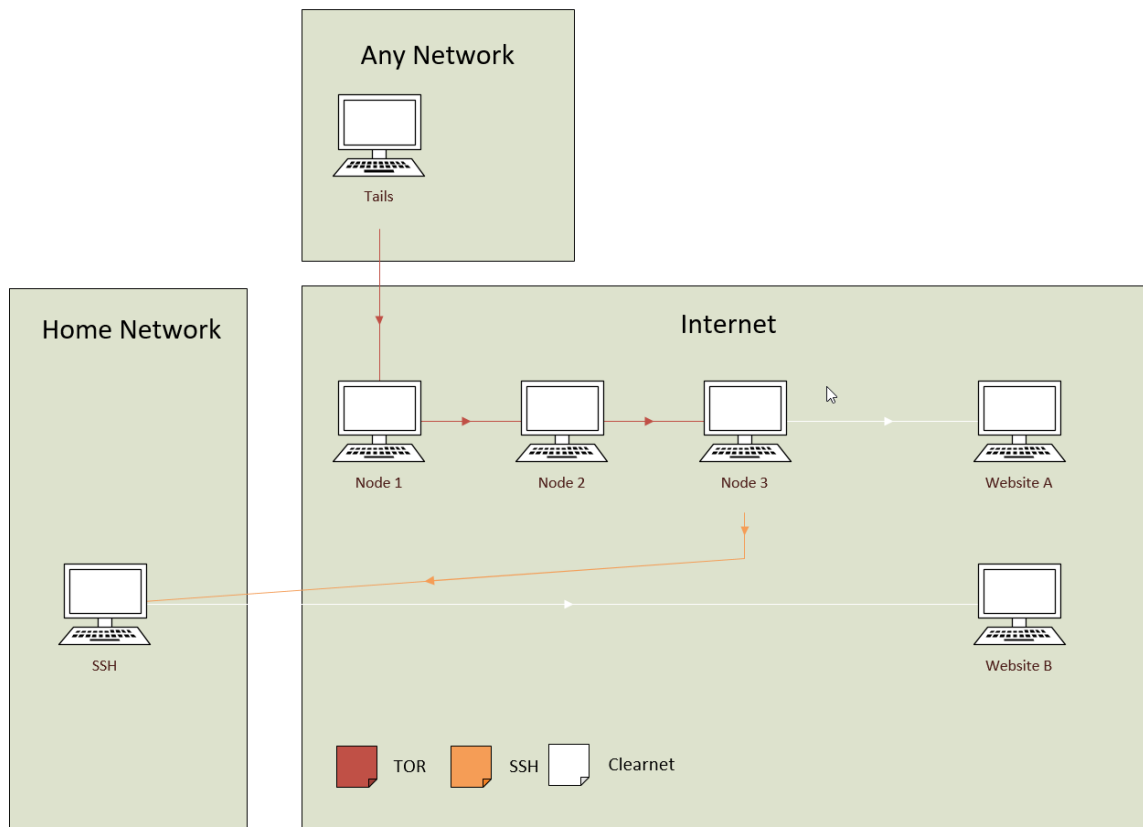
If you would like to connect to your personal home ssh server externally from the Internet with Tails, there is some additional work to do.

- Port Forwarding of TCP port 22 (or any other desired port you would like to use) to the destination IP inside the home network needs to be enabled. This has to be done inside your router or firewall, depending what device you are using to connect to the Internet. Most users own a router for connecting to the Internet. Please consult your router manual for the correct implementation of Port Forwarding for your device.

- In the same moment you are making the internal ssh-server reachable over the internet by Port Forwarding, there are some very important settings for the ssh-server that should be done prior to install and activate Port Forwarding on your router. All the recommended security settings for the ssh-daemon are stored in the file /etc/ssh/sshd_config.

- Do not allow root Logins over SSH (PermitRootLogin no)

- Allow only a single user to login over SSH (AllowUsers freaky)
  In the above example only the user "freaky" could make a ssh-connection to the ssh-server.

- You may not use the standard TCP port 22. A very good replacement port would be TCP port 443 or 53.

  Port 443
  Port 22

  In the above sample setting for sshd_config , the server would listen on port 22 and 443 for incomming ssh-connections. You could use port 443 from remote locations and at home port 22. Because you don't use port 22 from remote locations, you have less evil visitors that try try to break into you ssh-server.

- Only allow a ssh login with a key instead of a password. As long you don't have a user-key use this configuration inside sshd_config.

  PubkeyAuthentication yes
  PasswordAuthentication yes

  As soon, you can login with a valid key please change the value to:

  PasswordAuthentication no

  Or would you like to have not so nice intruders on your personal ssh-server from China and Russia that are trying to guess your root password the hole day long ? This is specially true if you are using the standard port 22 for SSH.

- Only use SSH-V2, The older protocol V1 shouldn't be used anymore.

  Protocol 2

- Fake the login message to mislead the snoopers or any disliked person.

- Put the SSH-daemon on a schedule, if you know you'll want it before hand.

- Always update your system to the latest versions available because your computer could be contacted directly from the Internet.

- Your computer at home needs to be up and running all the time. if you want to contact the your home server from any location via the Internet.

- Enable a DYNDNS name for your WAN IP, because most ISP's don't provide fixed IP-Addresses for the customers WAN interface. If you need a DYDNS name for your connections to the home network, I would call it a security hole that your often not aware of. On of the best and securest DYNDNS provider you find here.

  https://www.dynu.com/

I would like to emphasize the importance of the fact, like in the previous scenario 01, all traffic that you send out over my script can be traced by your home ISP or a local government. If you are placing a server like this in a company environment, the staff of the involved company could also be tracking all your traffic that you are sending over tails with my script. This is of course only true for the traffic that leaves the SSH-Server into the direction of the Internet. The traffic that crosses the 3 nodes into the direction of internet is encrypted and save !

4.0 Using a remote SSH-server anywhere on the Internet (best scenario possible)

Scenario 03:
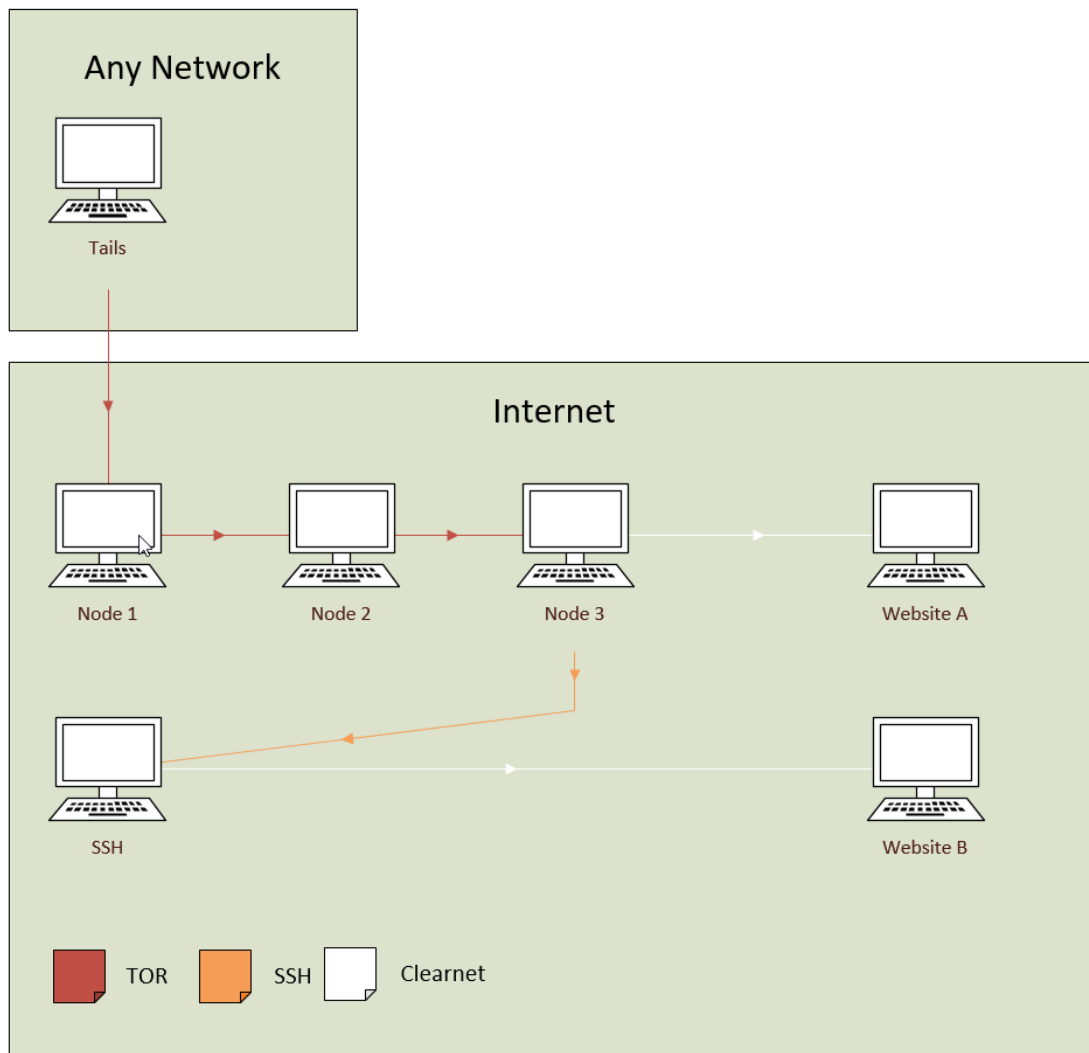
As you may now see, there are so many things that have to be configured correctly with SSH, especially if your own SSH-server can be reached from anywhere other the Internet. If you don't have a second computer inside your own network, the only suitable solution would be to find an SSH-provider anywhere on the Internet. This third option presented is the best option for all possible solutions to build your SSH-connection externally from Tails.

The difference from this Scenario 03 compared to the two previous presented scenarios, is that your currently used ISP can only see the TOR traffic to the Internet. To be a bit more precise, your current used ISP can only track the connection made to the first Node (Node 1) of the chain. Because all this traffic is encrypted, the ISP can not see what you are doing.

Every TCP packet you send to through the Internet passes through 3 different nodes until it reaches the desired destination. During this even the complete communication between the Node 3 (Exit-Node) and the foreign SSH server is encrypted by SSH until your packets have left the SSH-server. With all the above described scenarios , one thing should highly emphasized.

You can't hide the fact, from your currently connected ISP, that you are using the TOR-Browser or even Tails itself. If you really want to hide the fact that you are using TOR or Tails, you have to start with "Bridge Mode". If you are coming from the Big Brother County China, this is may the only possible way that Tails OS would working. If you are using only the TOR-Browser Bundle (not the Tails OS) inside of China with Windows or Linux , there is a other possible way to hide the fact, that you using the TOR-Browser.

[PC-OS → VPN → TOR→ CLEARNET INTERNET]

But this working CHINA scenario is not part of this manual, it only covers the Tails OS and this add-on. This add-on makes it work in a completely different way, you can see in the following illustrations.

[TAILS-OS → TOR → SSH → CLEAR INTERNET]

In most western countries it isn't necessary to hide the fact we are using Tails or TOR-Browser. Our ISP's or our current network operators can only see that we're using the ONION-Network , but what we are doing exactly is a mystery to them. They can even store all the traffic data we create, the only thing they are able to see is the IP of the node 1 we are connecting.

There are may cases like the one of the person Kim Eldo who thought he was making an "anonymous" Bomb threat to Harvard University.

https://www.dailydot.com/unclick/tor-harvard-bomb-suspect/

He was caught for just a simple reason. At the time the threat was created , he was the only person connected to the campus network that was using the TOR-Browser. It is only a guess from me but he wasn't using the Tails-OS that scrambles the real-MAC Address of the computer he used to create his threat. With the stored and detailed logs from the DHCP Server and the computer with the corresponding MAC address, it was easy for the authority's to catch him within minutes. According to the above article. Kim currently faces up to five years in prison with fines of up to $250,000.

- Start Tails in "bridge-mode"

In this new startup dialog of Tails (introduced in Version 4.20 and higher) , you can choose the second option start Tails into the "bridge-mode". To be honest, personally I don't like this window on startup of Tails.
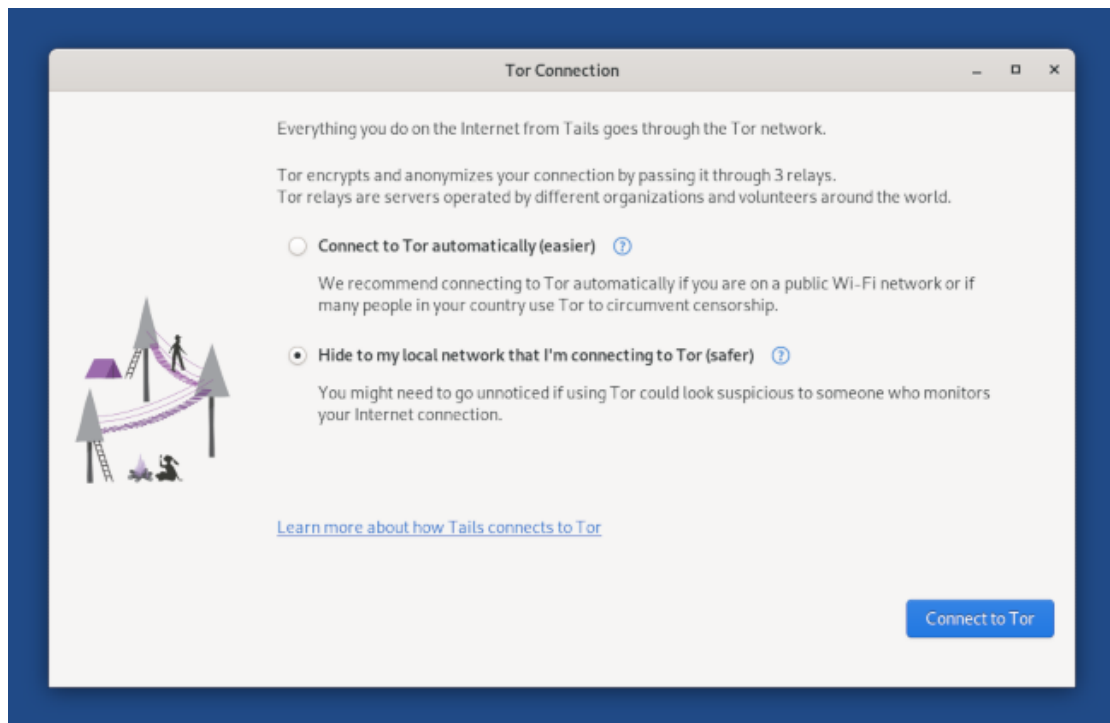
If you need more specific information about the bridge-mode of Tails, you can visit this following URL from tails.

https://tails.net/doc/anonymous_internet/tor/index.en.html

So where should you start looking for a public SSH-server on the Internet ? As a good recommendation and starting point, you should have a look at the following URL :

https://aruljohn.com/freeshell/
https://www.xshellz.com/

Once again, we emphasize that you should only visit these multiple websites in the above link with the Tor-browser of Tails. If you are visiting them with a normal browser on Linux or Windows to register, you may have already gone a step to far to hide your personal information.

A great piece of advice from me is to use a fake-email address to register for a SSH-service of your choice. I'm sure you will find many SSH-providers on that list that meet some or all of your current requirements for a good SSH-provider. And as a third and last piece of important advice from me, never create a username for a login that could be traced back to you.

- Some of them are free of charge, others are not.
- The process to create a valid account depends from server to server.

   - The only thing needed to create a account is a e-mail account.
   - A Email and a written postcard.
   - A little riddle to prove your knowledge about Linux and Unix in general.
   - Some hosts (blinkenshell.org as a bad example) would like to know your cellphone number to register. We don't even think about to give away any cellphone number only to register.

- Some of them don't ask for personal information about you, others would like to know almost everything about you. My simple advice is, use "Jon Miller / New York / USA" as provided contact information.

- Not many providers from that daily growing list, give a full shell-account including a new email address or the option for X11 forwarding. If you read the F.A.Q inside the doc directory, you may find a little hint placed by me.

- A few Servers only allow the creation of a socks5 server. No interactive shell (like bash) of any kind can be used.

- Many of them provide a little space to host a small website on the server.

- A few of them have databases like mariadb or mysql that you can use.

- The provided disk space to store personal files is very often limited to between 20 MB or even less. I know of only one SSH-Provider of that list that has a generous size of 20GB for a single user to use.

- Some of these listed SSH-servers would work very well, as long you aren't trying to connect to them over the ONION-network. At the same time you're trying to login over a public exit node 3 from the ONION- network to that SSH-server, they terminate the connection immediately. Like the Tor unfriendly websites we have already talked about, these servers are aware of the fact, that we are connecting to them over the ONION- network.

But wait, Yes ... there is a nice and clever solution for this little handicap. First we'll make an SSH-connection to a server that allows us to connect over the ONION network. From our first so called SSH "Jumpserver" we make the desired connection to our second SSH-server. The second server cannot know about our first ssh-connection, that we made over the Onion-network. Not very easy to configure, but it will work like a charm.

Most shell-providers of the provided red-pill list do not allow the following "bad things".

- Only allows exactly 1 active Connection with one registered login. Multiple connections with the same login would be detected and the user would be banned immediately after the second login appears.

- The installation of your own software or malware files is strictly forbidden.

- The use of popular port-scanners like nmap against other servers on the Internet is forbidden on most servers on the "Red-Pill" List.

- The use of software like "P2P" or "Torrent-clients" is strictly forbidden.

- On some servers is Internet Relay Chat (IRC) allowed, on others completely forbidden.

- Some of these listed systems have hundreds of active users so be nice and keep in mind that there are other users as well, so don't use up all the resources of the remote server. Like CPU, Memory, Disk space or even Bandwidth.

In the special circumstance, that you are a very experienced Linux administrator who doesn't trust anyone from the shell-list presented, you can use your own virtual Server for a low price on the Internet. I found a company in Europe that sells virtual Linux computers for only 4 Euros a month. This is a hard road to go down and not really recommend for a Linux novice or beginner, just one little mistake in your configuration, or the firewall design and the server will be hijacked within minutes after starting up the first time.

https://www.arubacloud.com/vps.aspx

If you have the required skills and the right motivation to secure this Linux server, ... you may have found your right server. But one thing is for sure … If you would go this way, you learn a lot about Linux and security.

To run this script from version 0.90 or higher you need at least the following things.

- One USB drive with at least 8 GB capacity. Please use a very fast drive for the installation. In the past I used some slow drives for Tails … what I never would do again !
- A current Tails version Version 7.2 or higher installed. Tails has an excellent documentation for the installation process itself.

  https://tails.net/install/

And here you find the information to create the persistent volume

  https://tails.net/doc/persistent_storage/configure/index.en.html

Connecting Tails with a existing network

  https://tails.net/doc/anonymous_internet/networkmanager/index.en.html

The first thing that you will do after is to create the persistent volume of Tails. You can't run my addon without a persistent volume. To be clear,a persistent volume within Tails with the following 3 mandatory options activated is needed. Without these 3 options enabled, the add-on will not work correctly as expected. These 3 options are needed and not nice to have.

SSH Client

Additional Software
Install additional software automatically when starting Tails.

Network Connections
Save Wi-Fi passwords and mobile broadband configuration.
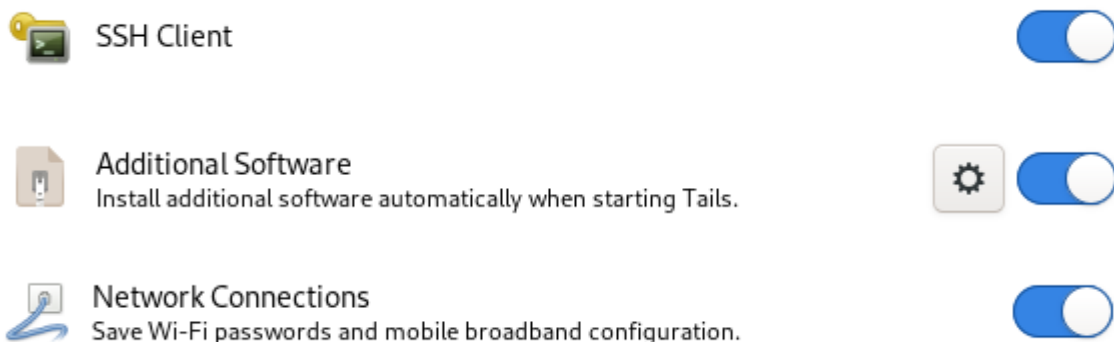
There are 3 various options more, that I highly recommend to activate !

Welcome Screen

Tor Browser Bookmarks

Dotfiles
Symlink every file in the Dotfiles folder into the Home folder.
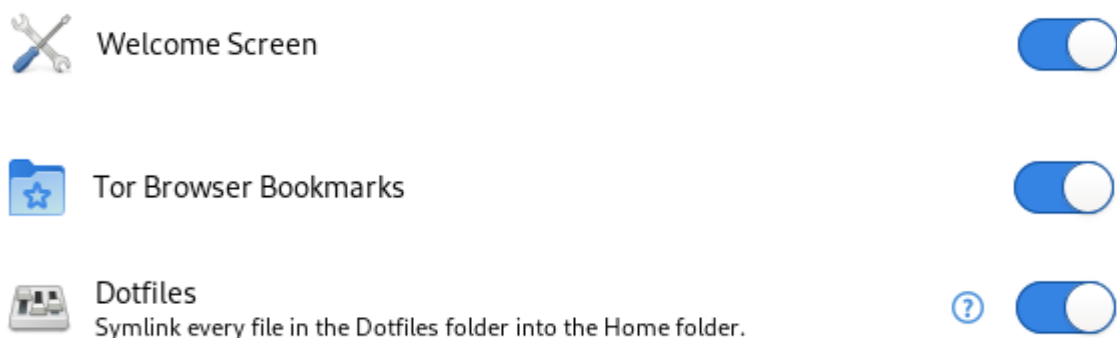
The remaining 6 persistent volume options available are :

- Persistent Folder
- Printers
- TOR Bridge
- Electrum Bitcoin Wallet
- GnuPG
- Pidgin Internet Messenger

If you use them or not, that depends on your own personal choice depending on how you use Tails. My add-on can also backup all the files of a persistent volume if you would like to do so. At this stage, from now on, please remember to do the following when you start Tails.

- You have to open the persistent volume on every start of Tails if you want to use the add-on. Of course, you can start Tails without the persistent volume activated, but the add-on itself and all the data that is stored on this persistent volume aren't accessible, even the stored WiFi passwords aren't accessible.

- If you are using special foreign chars for the password for the persistent volume, you have to set the correct keyboard layout first, otherwise you will be typing the password with the default English Keyboard (USA) layout in the Tails welcome screen.

- Prior to version Tails 4.12 it was not possible to store all the settings from the Welcome-screen. By now it is possible and I use it on every Tails OS I made for me or someone else.

- If you don't store the settings of your welcome-screen inside persistent, the administrator password for Tails needs to be set on every start of Tails. If you don't set the administrator password, the add-on won't be able to change the default local firewall. The script changes only one unique little setting inside the firewall of Tails. The changed setting of the firewall is very simple.

  sudo -S iptables -I OUTPUT -o lo -p tcp --dport 9999 -j ACCEPT

  This little change allows us to build a local socks5 proxy over SSH. Without this little modification, the predefined very tough default rules from iptables would block any connection attempt made to port 9999 from the internal loopback device 127.0.0.1.
  By now, it is not possible to use any other TCP Port than 9999 for the socks5 server.
  In a later release of this add-on, there a plans to make this port free changeable.

  We assume here, you have a working Tails disk and already created the persistent volume.

6.0 Installing the add-on

After the creating of the persistent volume you have to reboot to make the persistent volume active.
After the next startup of Tails you can change, the Language and the Keyboard layout:
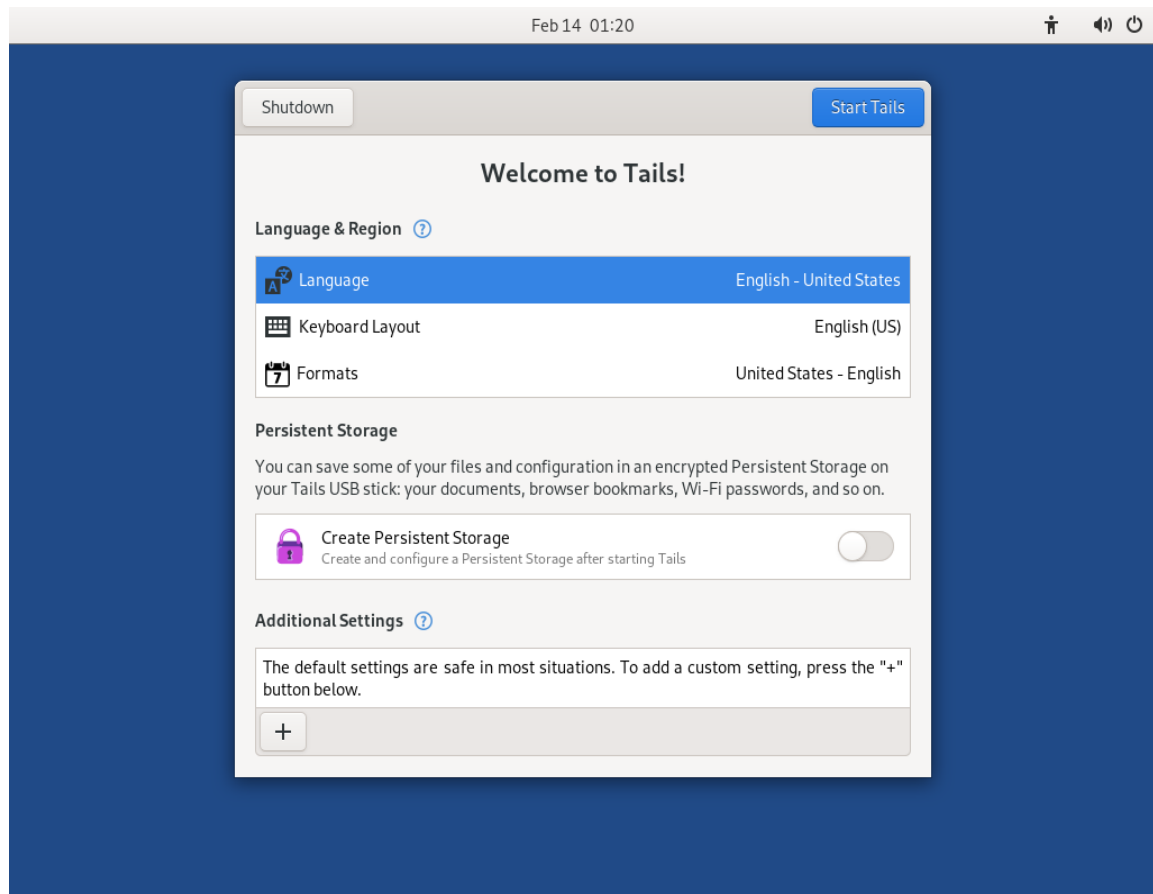
And then of course, you activate the persistent volume with the correct password.
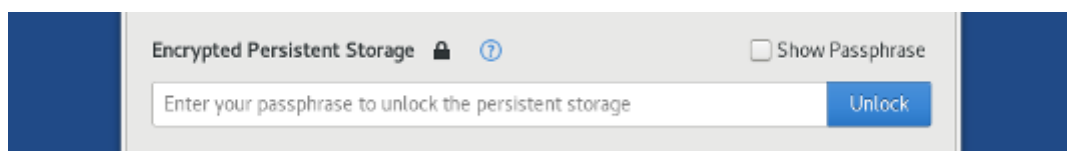
And as a last option, you set the administrator password and perhaps the disable "Unsafe Browser" inside of additional Settings as I already said.
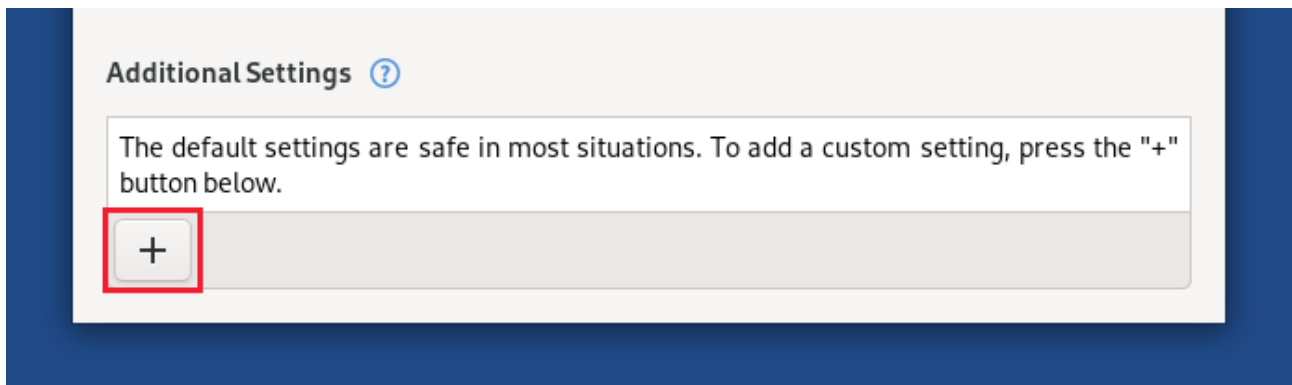
When you set the Greetings-Settings for the persistent volume to active, you only have to do this once, so as soon as you unlock the persistent volume on the next startup, all the values you stored here are loaded again, with the exception of the password for the persistent volume itself.

A little tip with the keyboard shortcuts on the startup screen of Tails :

Alt+K   Keyboard Layout
Alt+F   Formats
Alt+P   Persistent Storage
Alt+A   Additional Settings
Ctrl+Shift+A Administration Password
Ctrl+Shift+M MAC Address Anonymization
Alt+S   Start Tails

After successfully booting Tails the second time with the open persistent volume, please open a terminal inside the persistent folder, and then type the following command inside the terminal.
I explain you here, how you would do this.
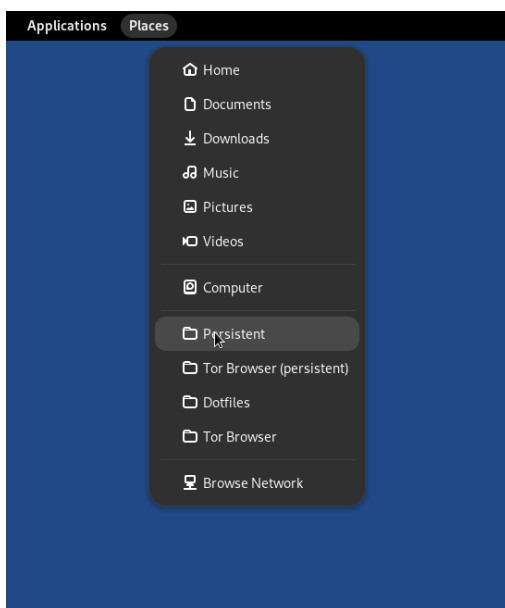
The Persistent volume contains in this stage only one single folder. Place the mouse pointer anywhere in the free area and press the right mouse button.
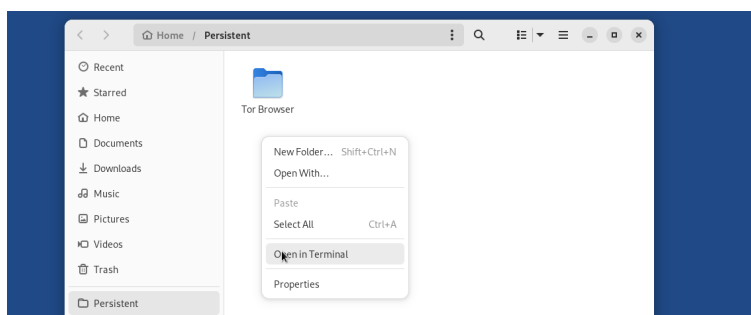
The linux-terminal opens here :
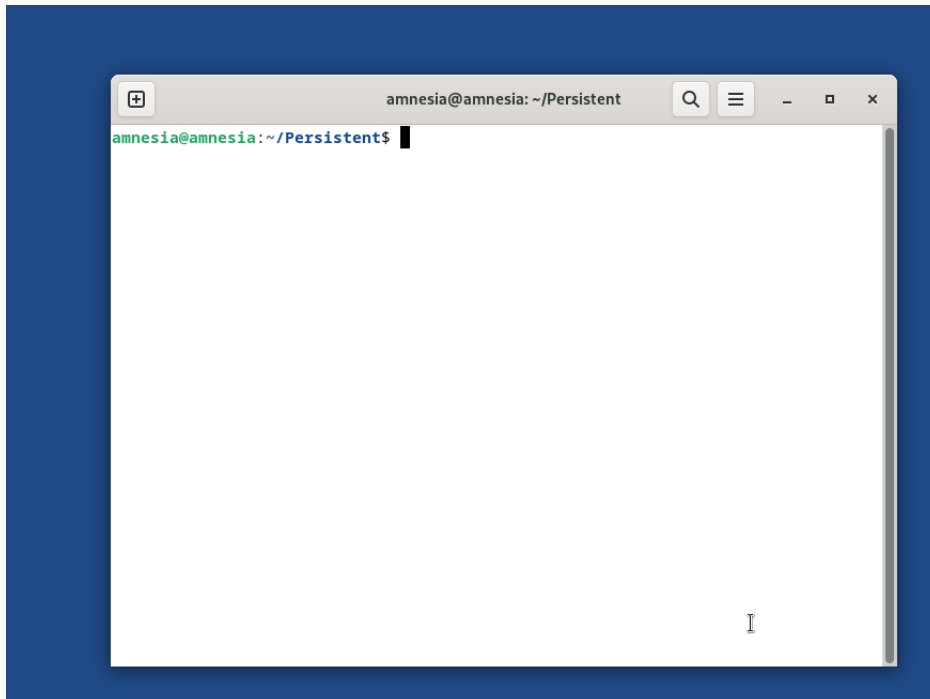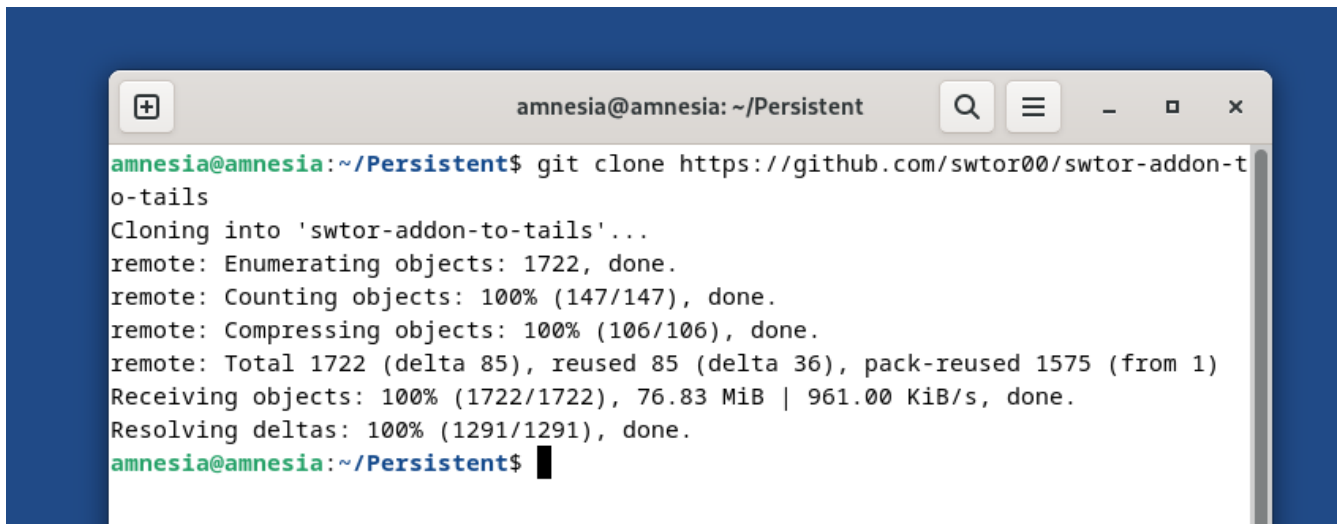
Inside this terminal,you have to type the following Linux command

git clone https://github.com/swtor00/swtor-addon-to-tails

Depending on the speed of your current Internet connection, after a while you should find a folder called "swtor-addon-to-tails" inside the persistent volume . Don't worry about the current connection you made to github (a microsoft company since June 2018). You are already using the onion-network from Tails in the background to connect to the public github-server and you are not leaving any traces or evidence on the github website that you are using this script or even Tails. (with the single exception of the public IP of the exit-node 3 that you are currently use).

If all goes correct, you should see the message like the following ones inside of the terminal.

By now you can close this terminal with the command "exit" or you can press <Ctrl>-<D>.

Before you do anything inside the directories of the add-on itself, you should first make a few very important decisions about the use of the add-on. The complete configuration of my add-on is written in a single file. It can be edited with the default Editor for Tails if you would like to edit the file this way in the terminal. Prior to executing anything, the complete path to this configuration file is as follows.

~/Persistent/swtor-addon-to-tails/swtorcfg/swtor.cfg

The default provided swtor.cfg configuration file (01.11.2024) over github for the add-on version 0.83 looks like this example right here.

```
SWTOR-VERSION:0.90
TAILS-VERSION:7.2
STATE: BETA
HOMEPAGE: https://github.com/swtor00/swtor-addon-to-tails
JOTV :
---------------------------------------------------------------
"La estupidez es una enfermedad muy grave ..."
---------------------------------------------------------------
OPTIONS FOR THE SWTOR-ADDON

GUI-LINKS:YES
BROWSER-SOCKS5:YES
CHECK-UPDATE:NO
BACKUP-FIXED-PROFILE:NO
BACKUP-APT-LIST:NO
TIMEOUT-TB:10
TIMEOUT-SSH:4
TERMINAL-VERBOSE:NO
CHECK-EMPTY-SSH:NO
AUTOCLOSE-BROWSER:YES
XCLOCK-SIZE:150
```

In the last few lines, you'll see all the relevant entries for the add-on configuration file. All the add-on options are written in CAPITAL letters. Let us now describe the settings that are possible in this file.

If you would like to check for an update on every startup of the add-on, you have to replace the following line containing the text

CHECK-UPDATE:NO with the new entry **CHECK-UPDATE:YES**

After this little change, the add-on contacts the github server that holds the master scripts on every startup to check if there is a new version to install. If you prefer to make this update check manually by yourself, please open a terminal and type the following commands.

cd ~/Persistent/swtor-addon-to-tails/scripts
./cli_update.sh

But I have to give you little warning about the use of the update-feature. This warning applies to both the updates possible (manual or automatic on startup).

Warning :

All local changes made to all files including the main-configuration file swtor.cfg are overwritten with the default values stored on the external github server. You have to re-apply all the changes you made again ! Of course only, if you made any changes to the configuration file swtor.cfg.

If you want to use the current script version without the tracking and control of the git software in the background, you could execute the following terminal commands to accomplish this simple task.

cd ~/Persistent/swtor-addon-to-tails
rm -rf .git
rm ~/Persistent/scripts/update.sh

At the same time you remove the .git directory from the add-on directory, you cannot execute ./cli_update.sh ever again.

GUI-LINKS:YES

If you change the value to NO, you can only start the script over a terminal. Most users should use the predefined default value YES. Prior to version 6.x it was possible to link a file directly on the Desktop of Tails. With the current Tails release 7.2 this is not longer possible. By now this entry defines, if my script install 3 additional entry's inside the Tails Application Menu or not, depending of this setting. If you leave it with the default value YES, the Tails-Menu looks like this.
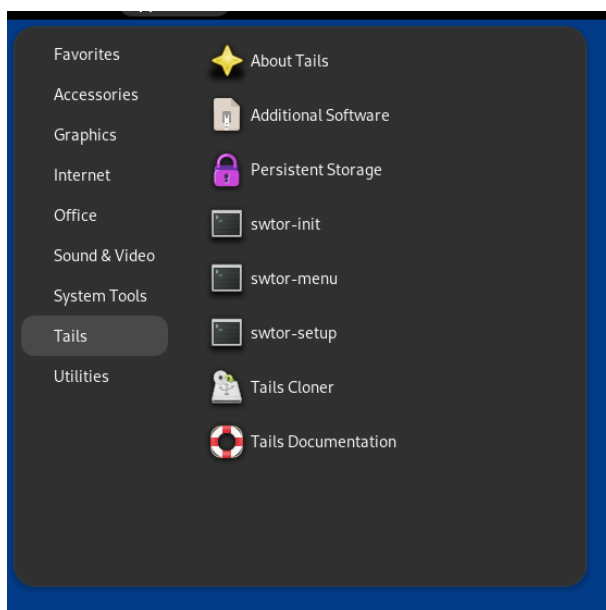
If you change it to **GUI-LINKS:NO** the Tails-Menu is not modified and remains untouched as it was. And you have to execute "swtor-menu.sh" on every startup over the GUI or in a Terminal.

BROWSER-SOCKS5:YES

Currently this entry should always be YES , In the near future it is may possible to use other settings like

RDP-CONNECTION / VNC-CONNECTION

BACKUP-FIXED-PROFILE:NO
BACKUP-APT-LIST:NO

If you activate both options to the value YES. What does this exactly mean to you as the user of this add-on ?

In the event that you would like to backup the complete persistent volume, the size of the backup will be around 500 MB or even more. If you leave the values at the default state NO, the created backup will have the size somewhere between 3 - 10 MB.

TIMEOUT-TB:10

This timeout value in seconds defines how long the scripts should wait until the error message that there is no active internet connection over the onion-network. The default value of 10 seconds should work fine for most users of the add-on. If your internet speed is very low, you may have to increase this value to 15 or 20 seconds until you get no more connection errors on startup.

TIMEOUT-SSH:4

This timeout value defines how long it takes to successfully connect to a remote SSH-Server.
If the timeout is reached and there is still no active SSH-Connection found, there comes a connection error displayed.

CHECK-EMPTY-SSH:NO

If you set this option to the state YES, on every startup of the add-on, the script is checking for a empty .ssh directory for the user amnesia. If you change this value to YES the startup of the add-on needs a few seconds longer than with the value NO.

AUTOCLOSE-BROWSER:YES

If there is a active SSH-Connection to a remote host and the are open Chromium Browser Windows the script closes all the open Browser Windows automatic. If you don't like this behavior, change the value to NO and all open chromium browser instances remaining open.

XCLOCK-SIZE:180

If you are using xclock to display the remote clock from a remote SSH-Server, this parameter defines the size in pixels. In case you desktop-resolution is very high (4k) you have to increase this value to something like 600 or 700 pixels to see the clock without the help of a binocular.

TERMINAL-VERBOSE:NO

If you like verbose output of the shell-scripts behind this add-on you have to set the value to :YES.

7.0 Configuring the required SSH-connection for the add-on

For this next configuration step, we need at least one valid SSH account from anywhere on the Internet or your own personal home-server. You may even first try to test this SSH connection with another operating system like Windows, Linux or even an Apple system which contains all the software needed to establish an SSH connection for testing purposes, generally all modern operating systems (including Windows 10 version 1803 or higher) have this SSH-software already included.

In my opinion, DO NOT even think about using this above discussed scenario. Under all circumstances, it's an insanely bad idea to use this SSH- connection anywhere outside of the Tails-system !! This is specially true if you are using a SSH-Server on the Internet !

If you really want to use a socks5 SSH connection to hide your browser traffic from your ISP with any other operating system than Tails, you should create a complete new login on a remote SSH-host only for that purpose !

If you would use these Tails only SSH-credentials outside of Tails, without the protection of the Onion-Network in the background, you would leak your currently used WAN IP-Address to the owner of the remote SSH-host immediately the moment you try to connect over SSH. A simple Linux command "who | more " inside a terminal of any user would list all the current connected users and the corresponding IP-Address from where the users are connected. An example output of the command could look this example.

eao	**pts/7**	**2019-xx-23 17:27 (85.220.101.10)**
dyama	**pts/8**	**2019-xx-25 02:07 (158.3.77.185)**
tt0077	**pts/9**	**2019-xx-25 20:08 (57.41.129.24)**

In the perfect case scenario that we are using the Onion-Network inside of Tails to establish the connection to our SSH-Server, the printed IP-Address for our username (column 1) in the column 4 would only be from our currently used Exit Node number 3. Otherwise it would be our real IP address from our currently used ISP. That would be very bad for our privacy we would like to protect. **Never mix up any SSH login credentials created only for a specific OS. Think about this twice before you do it !**

An SSH account with Linux or Unix normally consists of the following information for a successful connection.

- A username like digit1 without any spaces including a valid password or key-files.
- A destination TCP port. The default port for a SSH communication is TCP port 22.
- A valid DNS-Name or a IP V4 IP-Address to connect.

All the necessary configuration files for an SSH connection reside inside the directory /home/amnesia/.ssh. If this directory is empty, it means that we have never contacted any SSH-server before with our currently activated Tails system. To test our first SSH-Connection and see if we can successfully login over SSH, we need to open a terminal in Tails and execute the following command. You can replace the values in this example with the values provided by your own chosen SSH-provider.

ssh -p 22 digit@10.0.1.66

Let us see now , how this command is constructed.
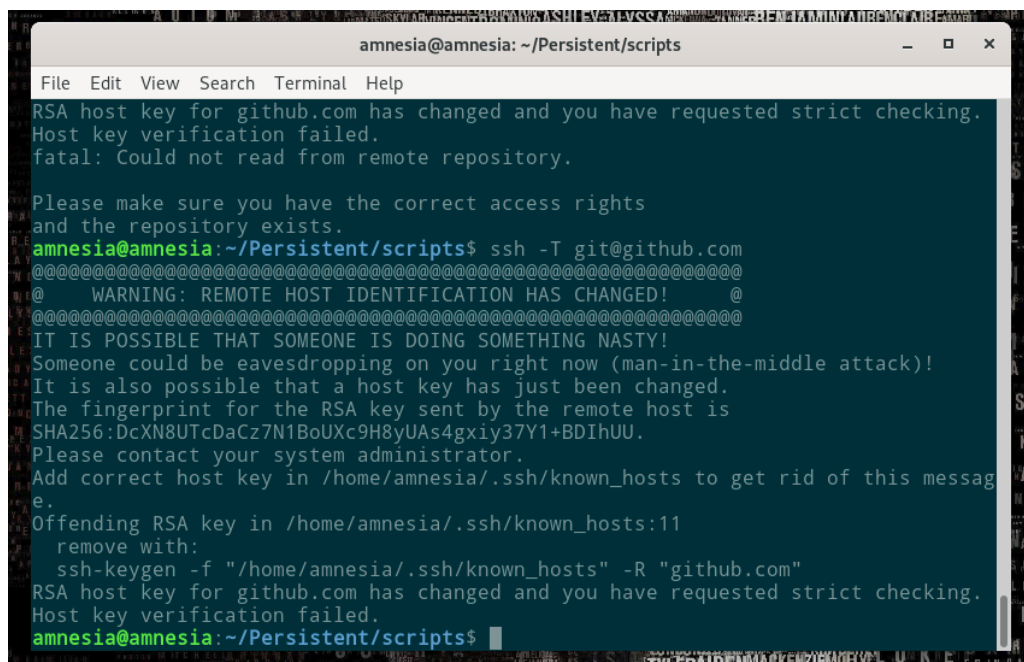
ssh	The local Linux command to communicate encrypted with the remote SSH-Server.
-p 22	22 is the default port for a SSH connection. Due to the default behavior of SSH , it isn't always necessary to add -p 22 for every connection. If your SSH-provider don't use port 22, then the -p XX (replace XX with Port from your Provider) option should be used every time you invoke the command.
digit1	The username for the SSH connection we are trying to establish.
10.0.1.66	The IP-Address of the remote server we would like to connect to. We could also provide a user friendly DNS-Name instead of a IP Version 4 IP-Address.

In case of the following scenario where we have never made an SSH active connection with our new Tails Medium, including persistent volume to an SSH-Server with the IP-Address 10.0.1.66, we will see a warning like following one.

The authenticity of host '10.0.1.66 (10.0.1.66)' can't be established. RSA key fingerprint is 90:8c:7a:f8:ae:1a:09:60:44:03:3b:d9:c9:f7:c4:76.
Are you sure you want to continue connecting (yes/no)?

This is the so called "public fingerprint" of the SSH-Server we are trying to connect to. The moment we type "yes" inside the terminal, the public fingerprint for this specific server 10.0.1.66 is then stored inside the file ~./ssh/known_hosts. After storing this public key inside of Tails, on every connection we make to the SSH Server 10.0.1.66, the already stored value inside the file ~/.ssh/known_hosts will be compared against the value that the server provides upon connecting. If there is a match of both values, we can continue to establish our secure connection.

If the two values don't match, then there is something really wrong ! If you find the following entries inside your log file or the terminal output like above showed, be very careful with your next action. This warning sign shouldn't be ignored never!

If the already stored puplic key inside Persistent and the offered public key from the remote SSH-Server don't fit together, we have to think twice about our next command. Please read the next URL to understand exactly, what could happen if you ignore this very important warning.

https://en.wikipedia.org/wiki/Man-in-the-middle_attack

- If you really decide to make the connection to this host anyway,then someone could now steal your current active password for that particular SSH-host or even worst, steal your currently used public SSH key if you ignore this very important warning and still connect to this possibly evil or nasty SSH-Server !!!!

- Or that the public key of the server has been replaced for some natural reason, possibly the remote server SSH-Server was replaced due to a hardware failure and the old already used SSH-Keys has never been restored.
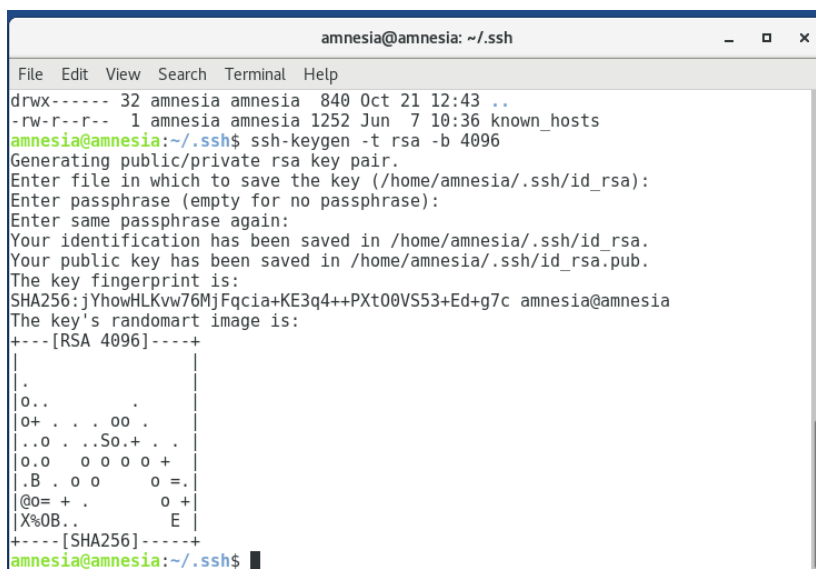
Next, you should see the password login, for the requested user login on the remote server. You can now type the password for that account and the remote shell should appear straight afterwards.

Please note that you can not see any char in the password field. Provided we can login to the remote server without any error, our next step would be to make this login password free in the future. We can close the remote shell on the remote server by typing "exit" or using the keyboard shortcut <ctrl><d>. Of course you could also customize a few things like changing the current password or a few other things. If you do change the current password, please write it down somewhere and store it in a safe place. If you have to start with a new empty Tails (Clean Tails Clone) , you may need to provide the password for the first SSH-Connection, to transfer the backups you made to your new installed Tails USB stick.

Our next terminal command is used to create the private / public key pair for all future SSH-communication inside of Tails. The command to accomplish this, is the following one :

ssh-keygen -t rsa -b 4096

After a short initialization time to generate these public and private keys , we have an output like the following one. This is now our own personal "holy-grail" of encrypted communication for the use inside of Tails and should be saved on a regular basis.

After the creation of our personal SSH-Keys, we can copy our public key to our SSH-server. There is a special SSH command to do this. This copy command will transfer only the public Key part to

the remote SSH-Server. The private key part remains in the safe hands of the persistent Volume inside Tails.

ssh-copy-id -i ~/.ssh/id_rsa.pub digit1@10.0.1.66

If the SSH-server isn't using the standard port 22, we have to add the -p X flag
(X stands for the port used by the remote Server) in the above sample. Some older Unix systems don't support the ssh-copy-id program, so with a few little bash-tricks it's possible to transfer the public key to the foreign SSH-server with the standard Unix commands every system should clearly understand. (Even the oldest ones ….)

cd /home/amnesia/.ssh
cat ~/.ssh/id_rsa.pub.pub | ssh digit1@10.0.1.66 'umask 077; \
cat >> .ssh/authorized_keys'

By now it should be possible, to make this specific SSH connection with Tails to the remote SSH-system 10.0.1.66 without any password or any other additional typing on the keyboard. We'll test the now SSH connection again by typing the following command.

ssh digit1@10.0.1.66

As you may have noticed, we did not use the flag -p 22 because this is the standard port. A full terminal from the remote host within your current terminal should appear without any password requested for the connection.

- For every single ssh-host you would like to connect to, you have to execute the command ssh-copy-id or you have to type the password again on every SSH connection you make !

- You should test every additional ssh-connection carefully so that there is no confirmation needed like adding the public key to the known_hosts file inside the directory ~/.ssh.

As soon as you have at least one SSH connection that works properly, you can create the configuration file that is needed by the add-on. Inside the "doc" directory of the add-on you will find a small example of this configuration file called swtorssh.cfg. All you have to do is edit the file with your own personal values and copy it to the proper location. The configuration of all possible SSH connections that this add-on can manage and use are defined in this single text file.
You have to copy the sample file from the doc directory to the correct location or to create a new file.

~/Persistent/swtor-addon-to-tails/swtorcfg/swtorssh.cfg

SSH itself is a very complex piece of software, if you would like to have more information about SSH in general or you need some cool advanced troubleshooting tips, you should have a closer look at using the TOR-Browser to navigate to the following URL.

https://annas-archive.org/md5/a422ecaeb30dab0547ce44134c07d24e

Some smart people call this reference book "The ultimate masterwork of SSH". If you have any problem related to the complex SSH in mind, in this book you will certainly find the answer to all of your current and future questions.

All SSH-connections made with the add- on have a "verbose" output on all actions. You will find all the verbose logs of SSH inside the following directory. The verbose mode of all SSH-connections inside of this add-on are made independent from the option TERMINAL-VERBOSE:NO or TERMINAL-VERBOSE:yes. The verbose logs are always generated.


~/Persistent/swtor-addon-to-tails/swtorcfg/log

If you have any connection issues, the first thing you should do is always have a closer look at the log-files. And please test all SSH connections you would like to use inside of the add-on carefully in a terminal. The SSH connection scripts work very well, but if you make any little mistake by configuring swtorssh.cfg then the add-on won't work like expected.

8.0 Execute Setup programm for the addon

For the last step open a Terminal inside ~/Persistent/swtor-addon-to-tails/scripts

./swtor-setup.sh

In the background this scripts only first checking that all mandatory parts of the Persistent Volume are activated. To do this internal tests we need the current Administration Password.
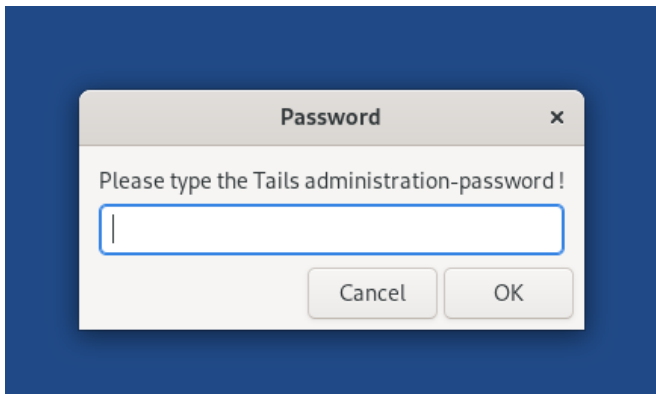
Typ it in and press OK. If you miss 3 times the correct password …. you have to start over again … The script can now test that :

• The SSH-Client Option is active
• The Additional Software Option is active

If there are no errors detected, the next window appear.
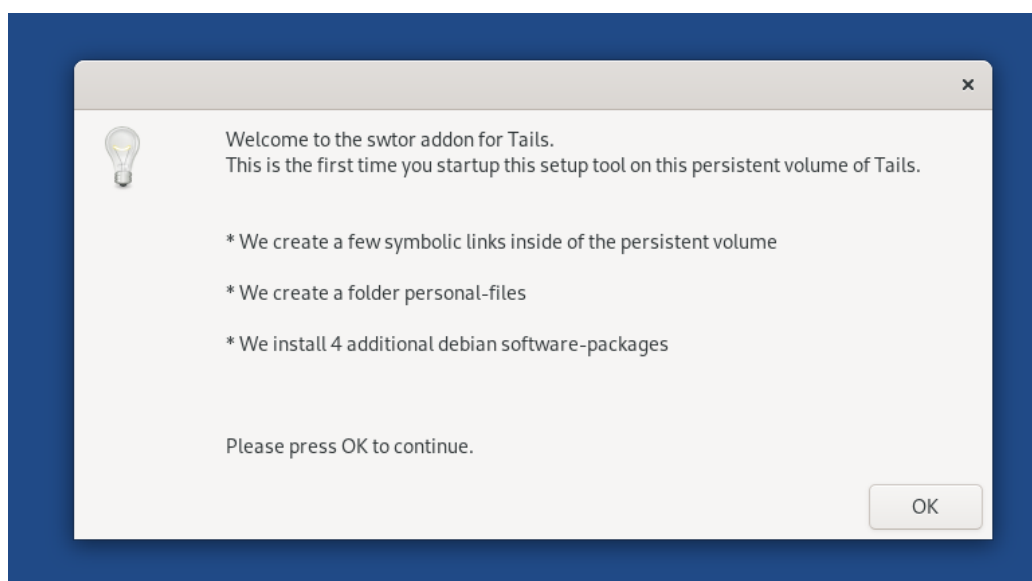
By pressing "OK" the scripts creates a few folders automatic inside of the Persistent Volume:

- doc (links to /home/amnesia/Persistent/swtor-addon-to-tails/doc)
- personal-files
- scripts (links to /home/amnesia/Persistent/swtor-addon-to-tails/scripts)
- settings (links to /home/amnesia/Persistent/swtor-addon-to-tails/settings)
- swtor-addon-to-tails
- swtorcfg (links to /home/amnesia/Persistent/swtor-addon-to-tails/swtorcfg)

The next step is to install 3 additonal debian packages that have to be installed on every bootup with Tails.

- chromium
- chromium-sandbox
- sshpass

You see the following Window :
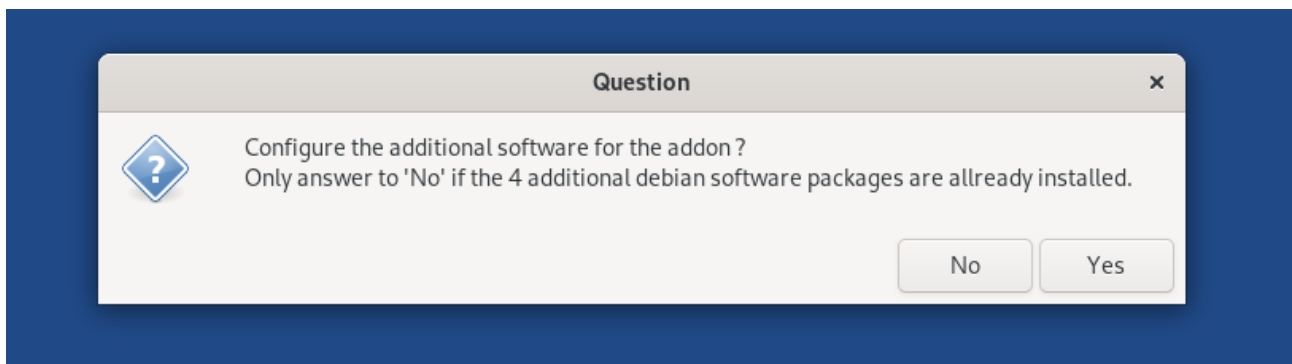
If you answer "Yes" the 3 above named software packages are installed. You have to confirm that all 3 packages have to be installed on every boot.

This command to install the software may need a long time …
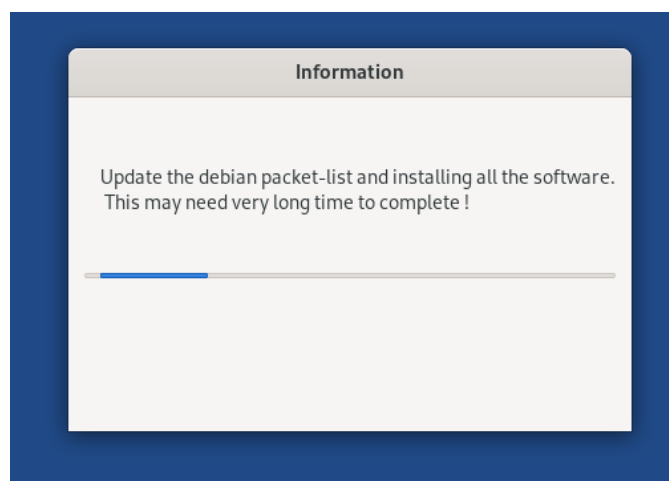
Please do not forget to mark the 3 additional software packages as "Install Every Time".

Below find you example, how this box looks with vlc-player
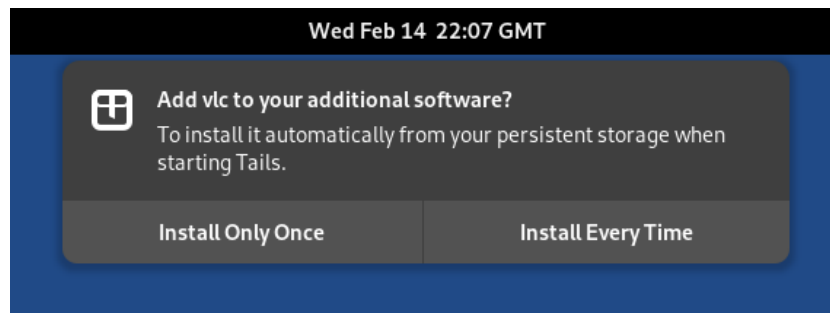
As soon the installation is finished ……. you see this and the setup is done.
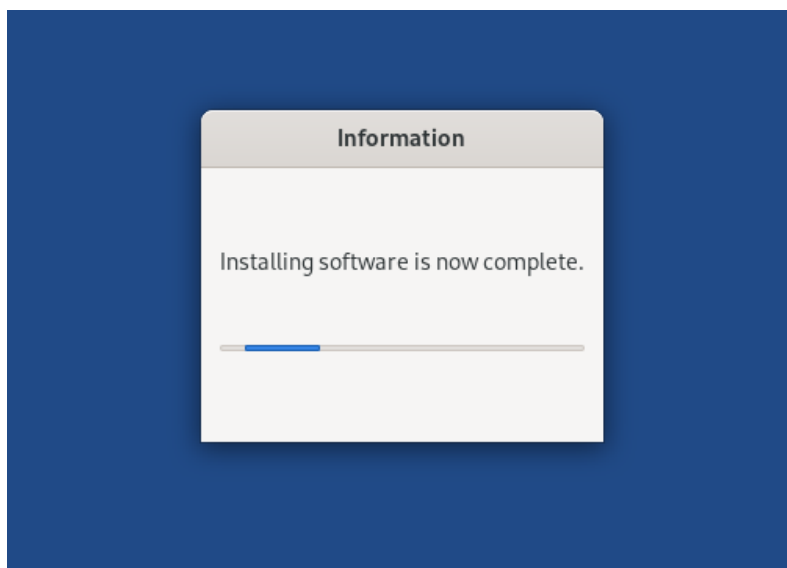
9.0 Execute the addon for the first time

After the execution of "swtor-setup.sh" I would make a reboot. On the next startup of Tails I would set the Administration Password including all other Settings that you like to wish .
After Booting navigate to the following folder :

~/Persistent/scripts

Open here a Terminal like you did it for the setup script in the last chapter 8.

Please type :

./swtor-menu.sh

After a few internal checks …. The following Window will appear, as you already saw it inside of setup script.
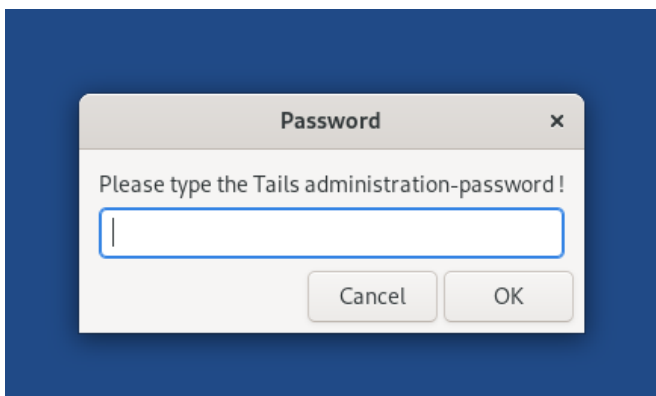
You have to type the correct Password and wait until you see this message :
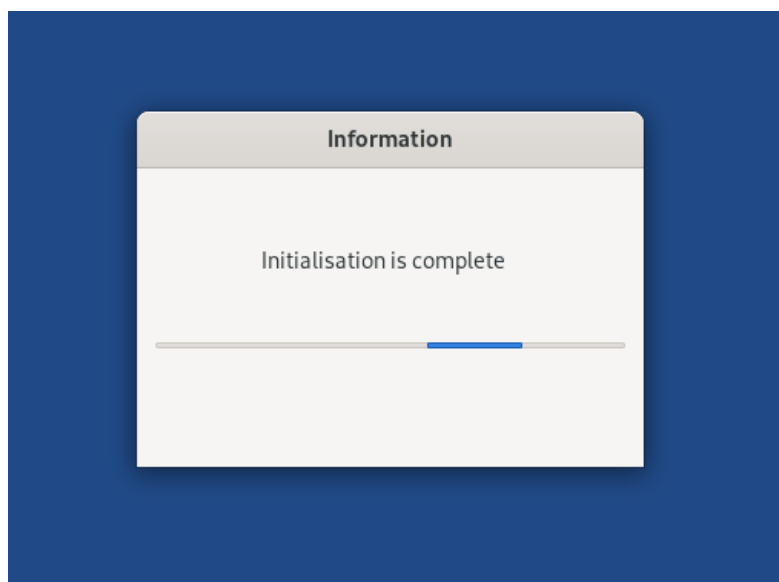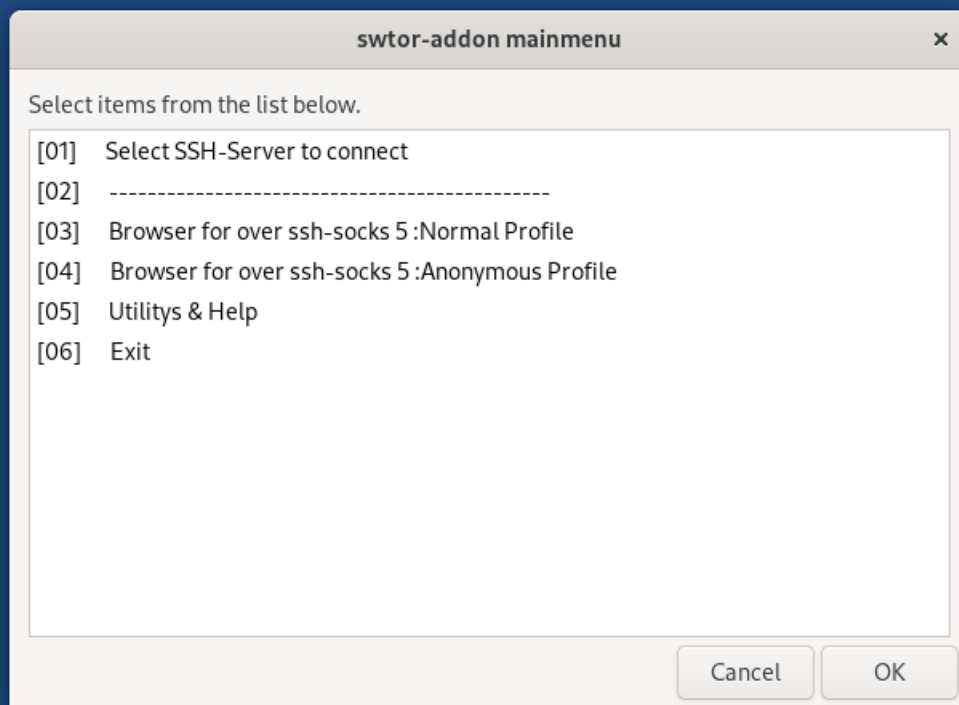
A few secounds later the main screen of the addon should be shown :

The first thing you should may do first is to select a destination Server by
cklicking on menupoint 01 → and "OK"

All your predefined SSH connections (swtorshh.cfg) are shown in a menu like this example:
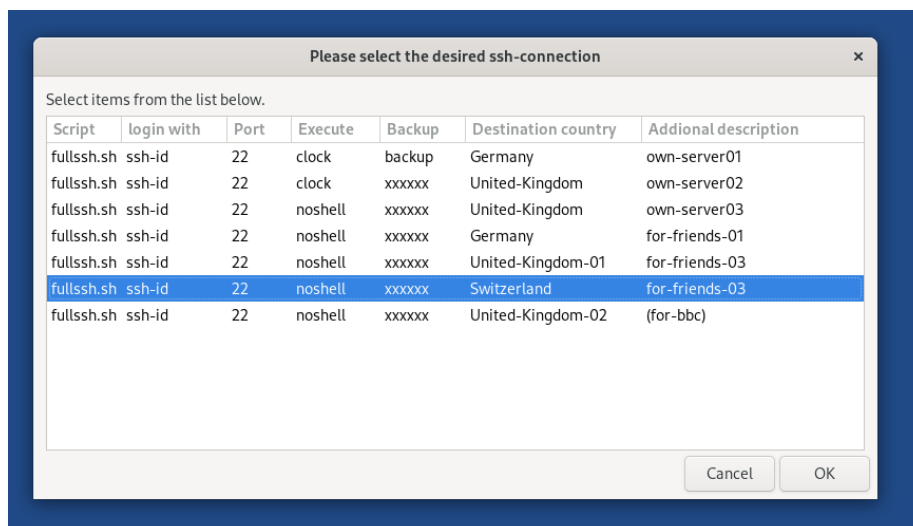
Select any line of the presented lines an press "OK" to connect to the selected remote Server.

If you have a connection without any error this window will appear :
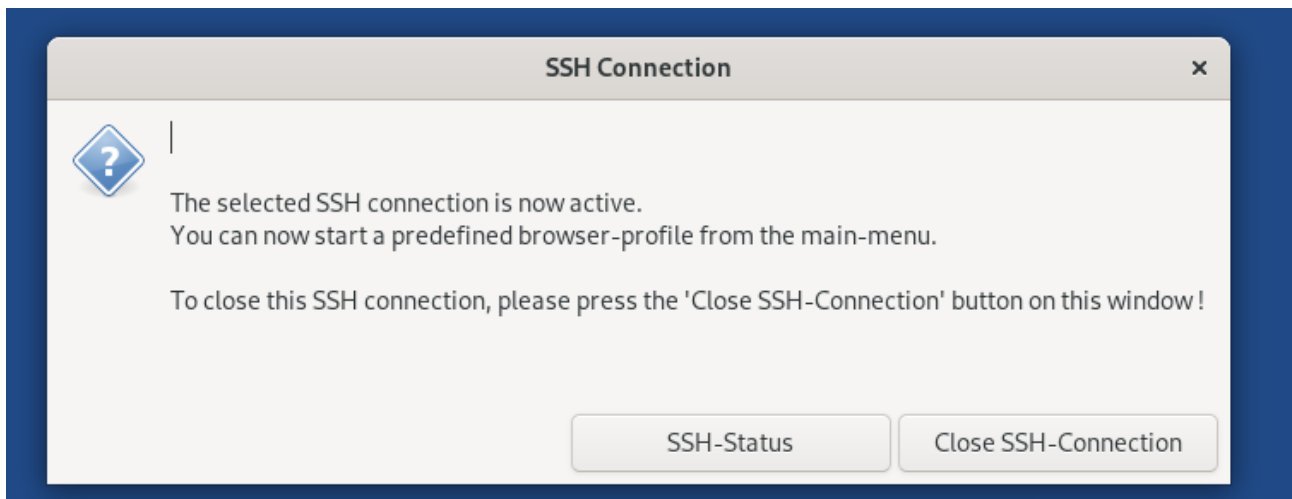
And a few moments later the main menu will be shown again. From there you select one of the Chromium Profiles.

The above Window remains open until you press "Close SSH-Connection" or the current sesscion closes unexpected !

If you have a error on the selected connection, you will see this and searching the failure :
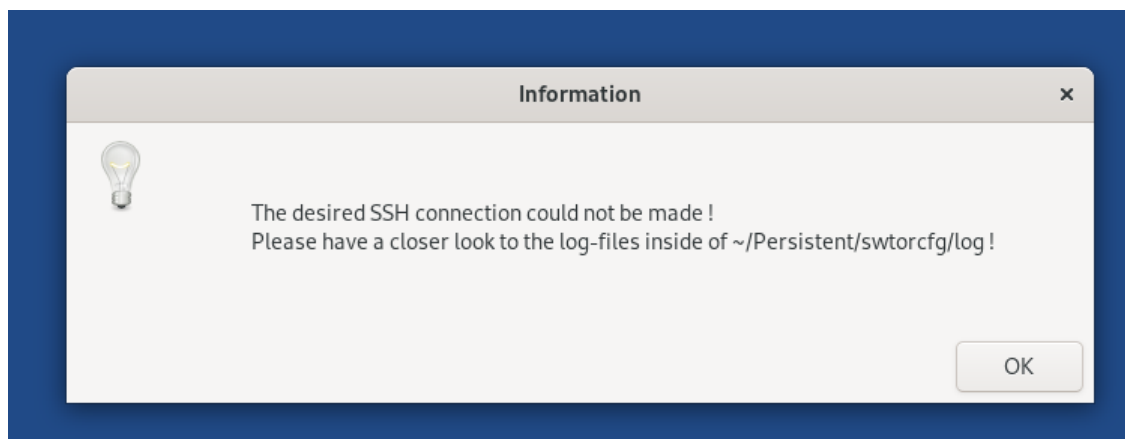
But the generated logs inside the directory ~/Persistent/swtorcfg/log are often the best help to resolve the problem.

- Did you ever contacted the selected SSH-Server and a Host Entry is missing ?
- You may have written the password wrong ?
- Is the user field and the server correct written in the configuration file ?
- Is the port number correct ?
- Did you made the transfer of the rsa-key ?

10.0 Tools explained → Freezing and Unfreezing

If you are open the Menu-Point 05 "Utilitys & Help" over the Main menu for the first time, you may ask yourself : What the hell is Freezing and Unfreezing inside the addon ?

Let us make a very simple and easy to reproduce example.
You are tired of the boring blue screen of Tails on Startup ?
You want to see on every boot the hidden files in file-manager ?
You would like to have a personal Desktop-Wallpaper ?

Without the so called freezing feature , you would have to set this settings by hand on every boot of Tails. You can use this nice to have feature only if your Persistent Volume have "DOT" Files activated. It will not work with deactivated DOT files.

Inside the script directory you find a example file called cli_tweak.sh. In the moment you executing this script , it will changes a few little things on the Desktop of Tails.

- Desktop Wallpaper will be changed
- Hidden files will be shown in the file-manager

and a few other little settings like disable Webcam and Mic

But this temporal changes are lost as soon you make a reboot of Tails. With the help of the freezing feature, you can save your personal configuration even after a reboot of Tails.

If you would like to have a configuration that you would like to keep after a reboot of Tails it is easy to archive this wish. The freezing of a current unfreezed System with all your current settings can be done over the add-on itself or over a terminal.

./cli_freezing.sh

It is highly recommended that you reboot Tails as soon as possible !

In the moment you are booting a freezed Tails … You can undo (unfreezing) all your freezed settings again over the add-on itself or with the inside the terminal.

./cli_unfreezing.sh

After the next reboot, Tails looks like it always was ….

Nice to know :

If you have the configuration "GUI-LINK:YES" and freezing a Tails System … In the next startup the add-on will be started automatic.

And of course as soon you are unfreezing the System you have to start it manual on every startup.
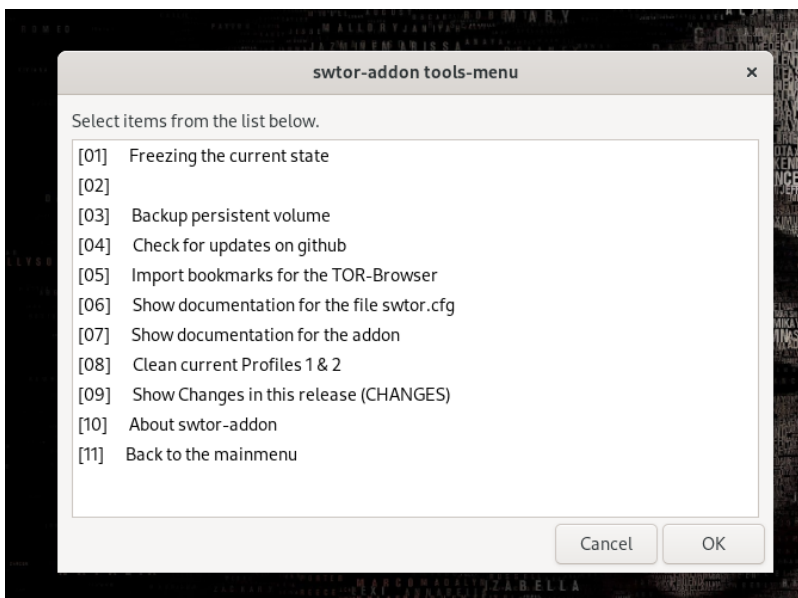
Note :

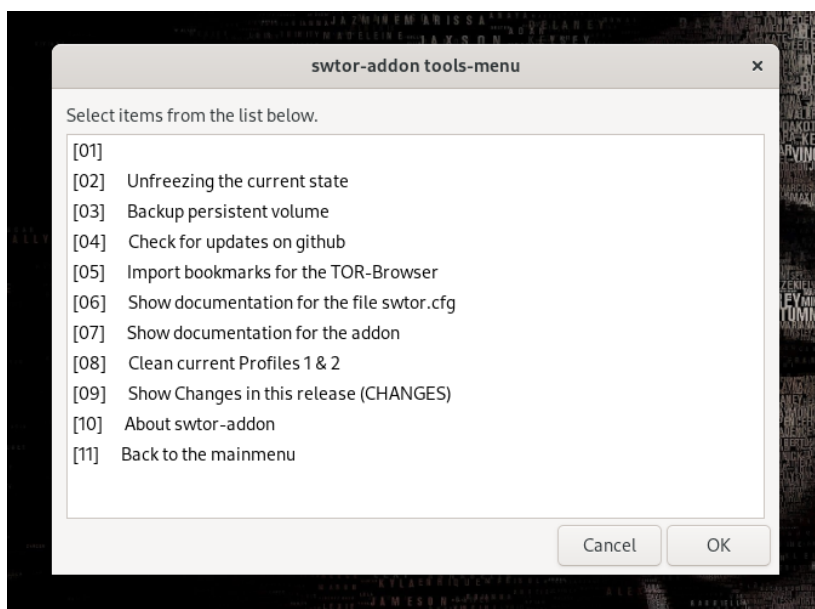Depending of your current configuration the Tools menu entry's looks different
If your current system can't be freezed (missing DOT on persistent), the menu looks like this.
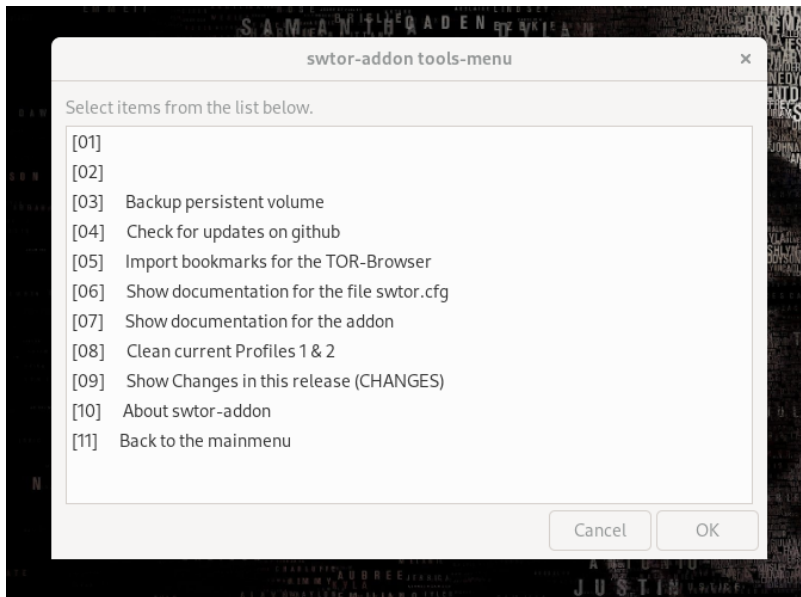
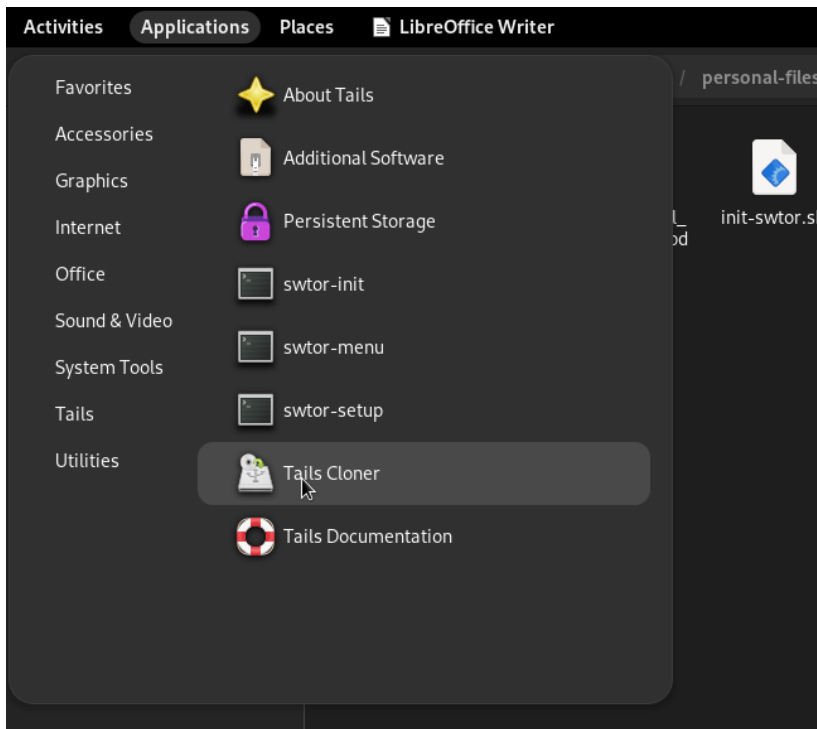If you could freezing the current system, this menu looks different :

And if your system is in the current state "freezed" your menu looks like this :

11.0 Tools explained → Backup

As you may have seen, Tails have a very good tool to create a backup (image) of the persistent volume.

To create a 1:1 backup to a other stick this tool is almost perfect. My backup script works in a different way. I create a tar.gz file inside the persistent volume with all the persistent options that are present during the backup. This generated tar.gz file could be encrypted and be send over SSH to a remote host.

What are the main differences between "Tails Cloner" and this backup provided in this tool ?

- The scripts backups all activated data from the persistent volume.
- The backup is protected against manipulations with a md5 checksum.
- The backup is very small and can be encrypted on demand.
- The following 3 folders are also included in the backup.

~/Persistent/personal-files
~/Persistent/Tor Browser
~/Persistent/swtorcfg

- The other addon directorys are not included in the backup → They are all restored from github

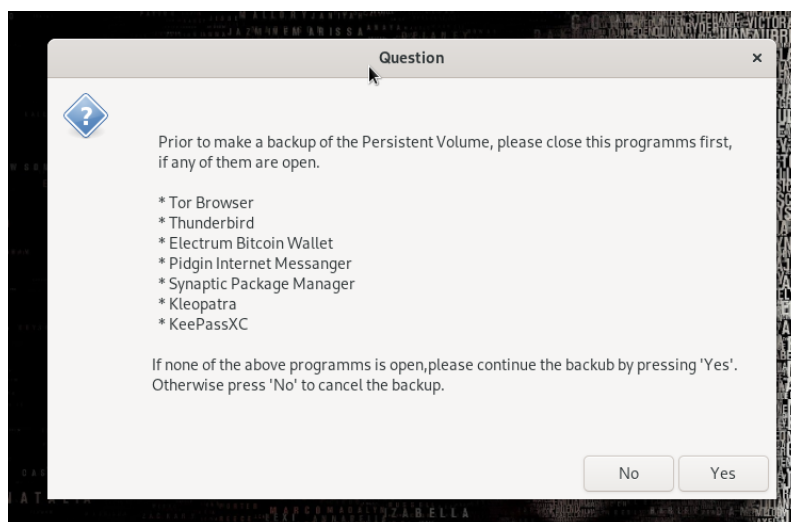All other exsiting folders on the persistent volume are not part of the backup !!!!!!

Where are the backup files stored ?

~/Persistent/personal-files/tails-repair-disk

If you would like to make backup, open the menu entry 03 inside tools-menu:
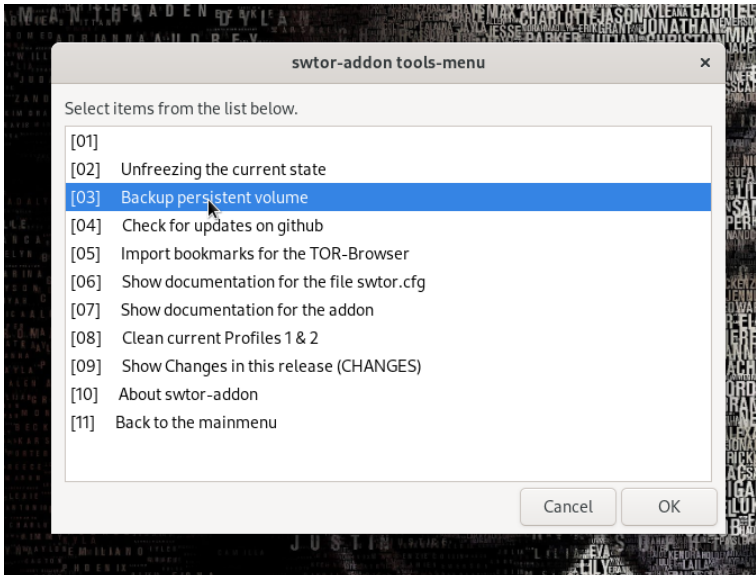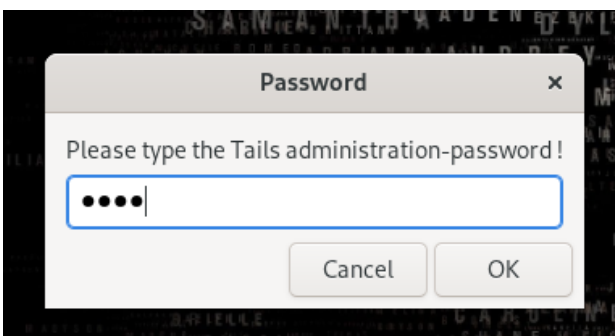

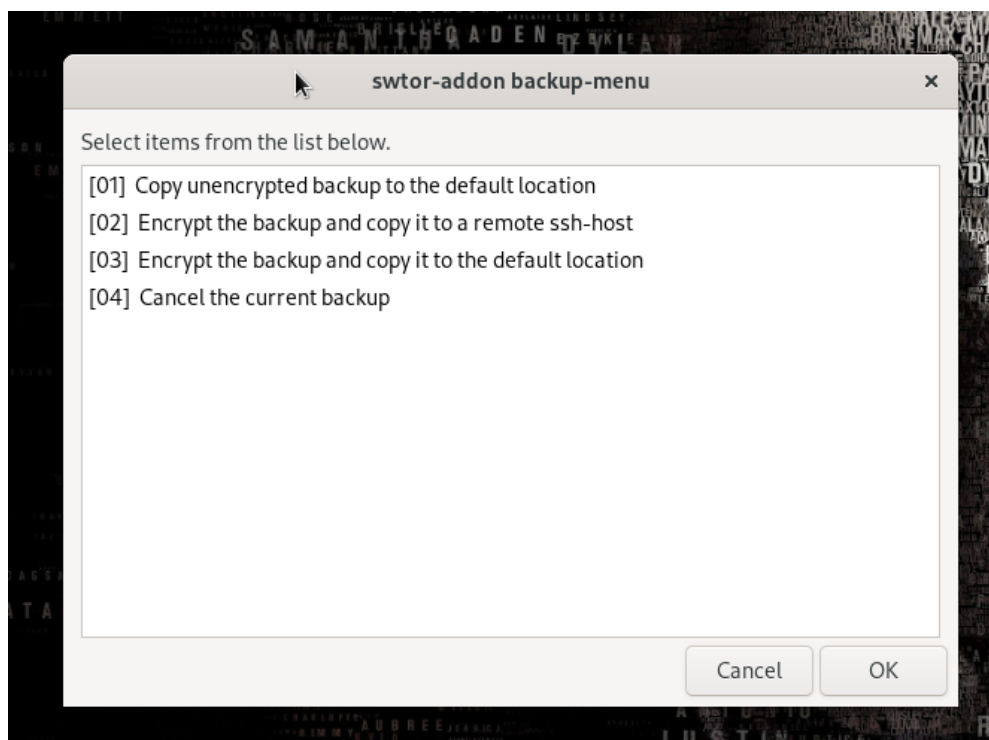After a few seconds this window appear :

If you press "No" the backup will be canceled. In the case you press "Yes" all the listed programs have to be closed first.

Later it will ask for the current administration password , as you already know it.

The backup starts now in the background. As son the backup is finished, you have to decide what to do with the created backup.
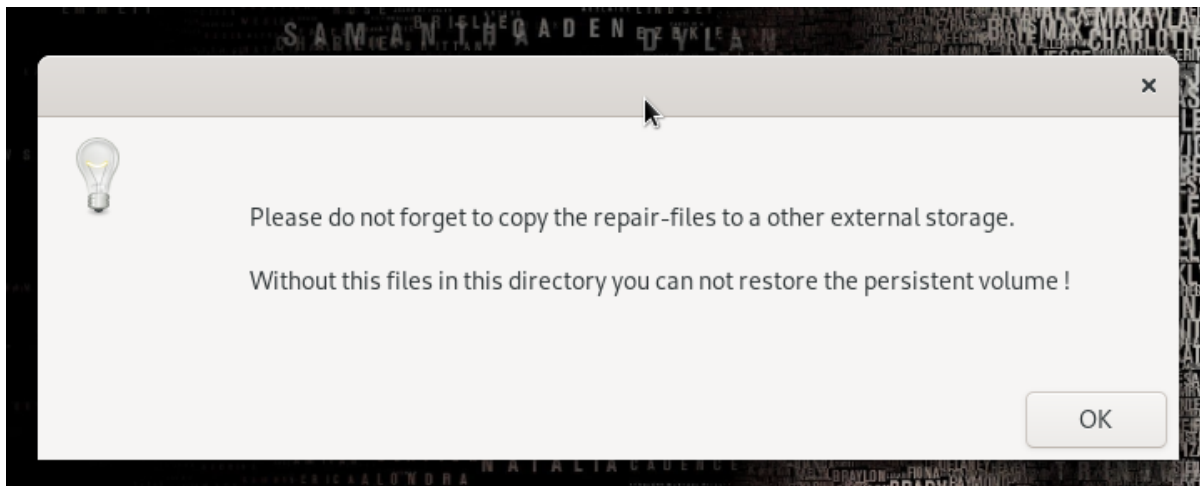

If you don't see the menu point 02 → You don't have a backup host defined inside the configuration file. But you can still encrypt the backup and store it inside your personal-files folder.

If you wish to encrypt the backup, the passphrase will be asked twice. And you see this following screen that contains the password.
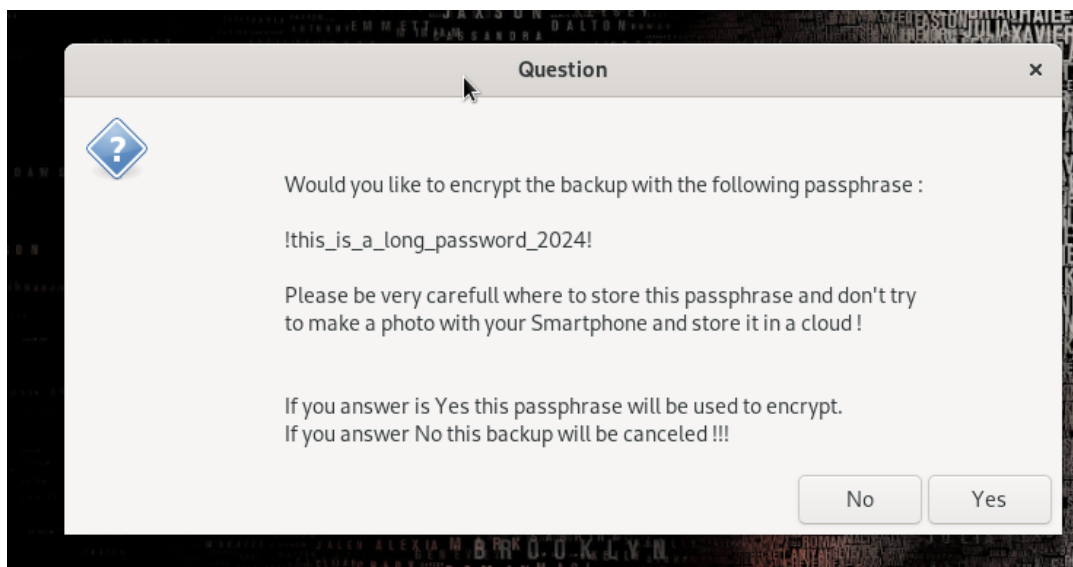
As soon the complete backups is finished, you see this little note to remind you to copy the files to a other place !

Please do not forget to copy the repair-files to a other external storage.

Without this files in this directory you can not restore the persistent volume !

OK

In the case the backup is not encrypted, you never copy this files to a location where it can be read by anyone who has access to this files.

- a other normal stick
- a remote ssh-host
- a cloud like Apple / Microsoft / Google

My advice where to store this files ?

Create a encrypted USB Stick with Tails and copy all files to this mounted volume.

12.0 Tools explained → Restore a backup to Tails

The restoring of the backup files in the chapter 11.0 described backup is very simple.

 Copy all files from the tails-repair-disk into a new Tails with a empty Persistent volume.

1.) Open a Terminal
2.) chmod +x restore.sh
3.) ./restore.sh

After a few moments → The restore is finished you can restart Tails.